

ARMY COMMUNICATOR

Approved for public release;
distribution is unlimited.
Headquarters,
Department of the Army

Voice of the Signal Regiment PB 11-12-3 2012 Vol. 37 No. 3

cyber defense

ENSURING NETWORK SECURITY ACROSS THE
FULL SPECTRUM OF MILITARY OPERATIONS

PLUS:

- New Chief of Signal Assumes Command
- 5 Key Cyberspace Defense Elements
- Elevated Offense Abets Cyber Defense



Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 2012		2. REPORT TYPE		3. DATES COVERED 00-00-2012 to 00-00-2012	
4. TITLE AND SUBTITLE Army Communicator. Volume 37, Number 3. Fall 2012				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Signal Center of Excellence, Army Communicator, Signal Towers (Building 29808), Room 713, Fort Gordon, GA, 30905-5301				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 52	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Continued Professionalism Assures Cyberspace Defense Dominance

Signaleers,

Greetings! First and foremost, it is an honor to be your 36th Chief of Signal. This edition of the Army Communicator provides a frank evaluation of where we stand in the on-going struggle for dominance in the domain of cyberspace. I encourage you to read this edition cover to cover.

Virtually everything in our environment from the power grid that brings electricity to the stove and refrigerator in your home to the ubiquitous cellular phones everyone carries depends on unencumbered cyberspace.

Everyday our military and domestic networks are constantly under attack from adversaries who seek to disrupt our use of cyberspace, deny our ability to use it or infiltrate our networks for intelligence.

The single greatest threat to our ability to maintain dominance in cyberspace is the education and training of our people. Being unaware of safeguarding techniques leaves room for both internal and external threats to penetrate and disrupt our critical cyberspace information infrastructure.

This fight over cyberspace includes every person who uses our networks, since we are only as strong as the weakest link.

The critical element in the equation is our people. I am confident in the professionalism of our Signal Regiment members to lead in this campaign to dominate the cyberspace environment and soundly defeat our adversaries. Our brightest

minds are on point in the midst of this on-going campaign and share some of their insights in this edition. We have a 152-year track record of consistently and unwaveringly "getting the message through." Through tough times and extraordinary transitions, the core values we stand on have distinguished us as **Army Professionals** and assured our successes.

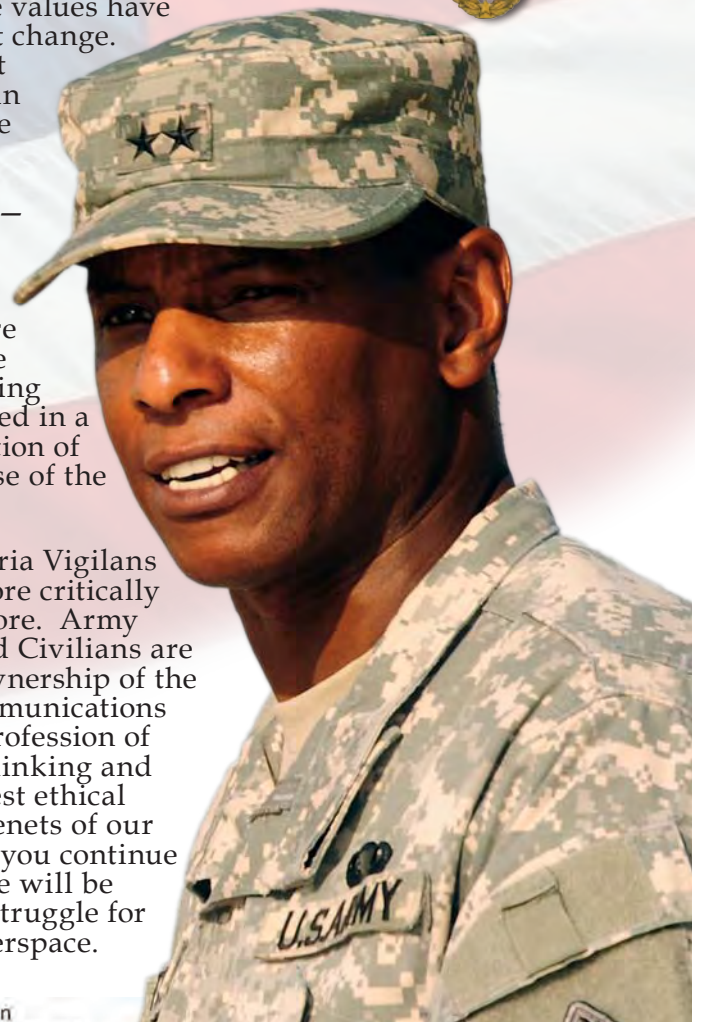
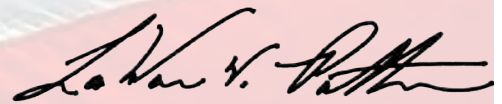
Today we are not only engaged "over there." Cyberspace extends to every corner of our homeland. Even though the battlefield has changed and continues changing, our core values have not and should not change. I am confident that we will dominate in cyberspace because every one of you—service members and civilians alike—know that we are involved as Army Professionals in a pursuit that is more than a job. You are called on and serving in a capacity steeped in a deep moral obligation of duty for the defense of the nation.

Our motto Pro Patria Vigilans rings truer and more critically now than ever before. Army Signal Soldiers and Civilians are charged to take ownership of the networks and communications systems and the Profession of Arms. Continue thinking and acting in the highest ethical and professional tenets of our profession. When you continue to do so, I know we will be victorious in this struggle for dominance in cyberspace.

As one **Army Professional** to another, I sincerely thank each Soldier, Army Civilian, sister service member and our Families for your commitment to our Army and our nation.

Pro Patria Vigilans

For the Country!



COMMAND

Chief of Signal

MG LaWarren V. Patterson

Regimental Chief Warrant Officer

CW5 Todd M. Boudreau

Regimental Command Sergeant Major

CSM Ronald S. Pflieger

EDITORIAL STAFF

Editor-in-Chief

Larry Edmond

Art Director/Illustrator

Billy Cheney

Photography

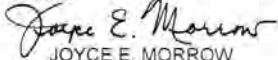
Billy Cheney, Marlene Thompson, Nick Spinelli,
Cotton Puryear

By Order of the Secretary of the Army

Raymond T. Odierno

General, United States Army
Chief of Staff

Official:


JOYCE E. MORROW

Administrative Assistant to the
Secretary of the Army

Authorization 1224009

Army Communicator (ISSN 0362-5745) (USPS 305-470) is published quarterly by the U.S. Army Signal Center, of Excellence at Signal Towers (Building 29808), Room 713 Fort Gordon, Ga. 30905-5301. Periodicals postage paid by Department of the Army (DOD 314) at Augusta, Ga. 30901 and additional mailing offices.

POSTMASTER: Send address changes to **Army Communicator**, U.S. Army Signal Center of Excellence, Signal Towers (Building 29808), Room 713, Fort Gordon, Ga. 30905-5301.

OFFICIAL DISTRIBUTION: **Army Communicator** is available to all Signal and Signal-related units, including staff agencies and service schools. Written requests for the magazine should be submitted to Editor, **Army Communicator**, U.S. Army Signal Center of Excellence, Signal Towers (Building 29808), Room 713, Fort Gordon, Ga. 30905-5301.

This publication presents professional information, but the views expressed herein are those of the authors, not the Department of Defense or its elements. The content does not necessarily reflect the official U.S. Army position and does not change or supersede any information in other official U.S. Army publications. Use of news items constitutes neither affirmation of their accuracy nor product endorsement.

Army Communicator reserves the right to edit material.

CORRESPONDENCE: Address all correspondence to **Army Communicator**, U.S. Army Signal Center of Excellence and Fort Gordon, Signal Towers (Building 29808), Room 713, Fort Gordon, Ga. 30905-5301. Telephone DSN 780-7204 or commercial (706) 791-7204. Fax number (706) 791-3917.

Unless otherwise stated, material does not represent official policy, thinking, or endorsement by an agency of the U.S. Army. This publication contains no advertising. U.S. Government Printing Office: 1984-746-045/1429-S.

Army Communicator is not a copyrighted publication. Individual author's copyrights can be protected by special arrangement. Acceptance by **Army Communicator** conveys the right for subsequent reproduction and use of published material. Credit should be given to **Army Communicator**.

ARMY COMMUNICATOR





Worldwide web homepage address
<http://www.signal.Army.mil/ocos/AC/>
E-mail: ACeditor@conus.Army.mil

PB 11-12-03
Fall 2012
Vol. 37 No. 3

Voice of the Signal Regiment

Table of Contents

Features

- | | | | |
|----|--|----|--|
| 3 | Cyberspace Doctrine Update | 34 | Citizen Soldiers defending cyberspace
MAJ Aaron Munn
John Galeotos |
| 4 | Chief of Signal Command changes
Wilson A. Rivera | | |
| 6 | Signaleer assumes four-star Command | 37 | Redefining Information Assurance compliance
LTC Christopher Quick |
| 7 | Operating on unconventional terrain
 LTC Michael Lanham | 40 | Certification hits the Jackpot
LTC Jan Norris
ILT Natasha K. Pennyfeather |
| 13 | NetOps here we come
CW5 Todd M. Boudreau | 42 | Configuring battalion file servers
CPT Matthew Sherburne |
| 15 | Studying Computing Offense
 MAJ T. J. O'Connor
CPT Ryan Hand
CW3 Matt McDougall | 44 | Signal classrooms embracing high technology tools
Nick Spinelli |
| 19 | Combined Arms Approach to network defense
Russell Fenton | 49 | Get the latest information on security training
<i>LandWarNet eUniversity</i>
LWN.ARMY.MIL |
| 22 | Five Key cyberspace defense elements
 Jac W. Shipp | | |
| 26 | Engaging two domain warfare
 LTC Christopher R. Quick | | |
| 31 | Rigorous cyberspace defense expert training advances
CW4 Ivory Torbert | | |

Departments

- 46 TCM Updates

Cover: *This edition covers cyber space defense as a critical issue with Signal Regiment leaders assertively moving forward to dominate this mission critical domain.*



Cover by Billy Cheney

Join the Discussion

At the end of articles where you see this icon,  you can weigh in and comment on-line.

Working to create cyber defense experts

Signaleers,

I have been looking forward to this edition of the *Army Communicator* because there are some significant questions we need to engage openly and honestly.

Everyone realizes that our Mission Command and network communications systems have grown in magnitude and complexity. It is not as apparent that there has been a shift in advantage from the defensive to the offensive. The historic degree of difficulty due to the complexity and cost of reverse engineering communications systems that were mostly proprietary was a huge barrier for our potential adversaries. That's no longer true. Today we use a plethora of commercial off the shelf equipment in the same manner as the rest of the world. This allows common universally applicable exploitation tools to be used against the U.S. Army.

Because of this massive shift in favor of the offensive (i.e., toward our adversary in comparison to our cyber defenders), can our cyber defense experts be expected to stop every attack? Think of it like this: do you expect even the best goalie to stop every shot at the goal? What if the oppos-

ing team has an unlimited roster of players on the field and each has multiple pucks that can all be shot at the same time. What would you expect to happen?

We are working hard to ensure we create the best cyber defense experts possible. We must take more of a holistic approach through sound principles of Network Operations.

Even though we have a NetOps construct, are we really conducting, or even able to conduct true Network Operations? Could it be that we merely stage a transport and routing architecture and then reactively optimize based on bandwidth demands? Could it be that we establish data services based upon a static model of Mission Command service expectations? Could it be that we systematically employ Information Assurance measures based upon forensics of successful CNE and/or CNA actions? What happens when the adversary moves from a CNE posture of data exfiltration to a CNA posture to manipulate data and/or to disrupt, deny, and/or destroy our information systems due to political or kinetic triggers?

Are we prepared to hunt for potential adversarial activity in accordance with an established playbook that includes immediate preemptive transport routing modifications; data screening, filtering, and transition to alternate servers (e.g., COOP); and ensure uninterrupted Mission Command Essential Capabilities while a near-peer adversary aggressively attempts to disrupt and/or manipulate our essential information and key Cyberspace terrain? In other words, can we conduct NetOps?

This and many other aspects of cyberspace defense are addressed in this edition. Additionally, we solicit your thoughts, expertise, and support in taking back the advantage though holistic, integrated, and synchronized NetOps functions.

As always, thank you for your dedication and service in being ever Watchful for Our Country.

Pro Patria Vigilans!



Todd Boudreau



Cyber defense generating doctrine changes

"We're focused on providing a professional team of elite, trusted, precise, disciplined cyber warriors who defend our networks, provide dominant effects in and through cyberspace, enable mission command, and ensure a decisive global advantage."

- LTG Rhett Hernandez

Commanding General of U.S. Army Cyber Command, 2nd Army
Army News Service, 26 July 2012

Over the past decade, the operational environment has changed dramatically and the LWN has become a critical part of that change. The Army depends on cyberspace operations, the GIG, and LWN NETOPS to defend our network. The defense of our network allows sustained operations in support of mission command to enable unified land operations. The DOD Strategy for Operating in Cyberspace established cyberspace as an operational domain which impacts Signal support to military commanders. As a relevant operational domain, cyberspace along with the GIG and LWN, must be defended.

The Signal Center of Excellence is developing FM 6-02, Signal Operations as the primary Signal doctrine reference. FM 6-02 will discuss how the Signal Regiment supports the Army's mission across the range of military operations. FM 6-02 will establish the Signal Regiment's roles and responsibilities of signal operations providing the essential capabilities that enable and support the Army's mission at all echelons. This includes the responsibility to defend our network within the cyberspace domain.

The DOD definition of cyberspace is "the global domain con-

sisting of interdependent networks of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers." The GIG, as the DOD part of cyberspace, links to national and global cyberspace and interacts with the national information infrastructure, and global information infrastructure respectively. The LWN is the Army's portion of the GIG.

FM 6-02 will discuss NETOPS which is defined as the activities conducted to operate and defend the GIG and LWN which contribute to the defense of cyberspace.

The Signal Regiment's core competencies define the Signal Regiment's distinct, unique, and valuable contribution in support of mission command to unified land operations. NETOPS is the Signal Regiment's core competency/critical task which supports defense of the LWN. The components of NETOPS are: enterprise management, network assurance, and content management.

Through the core competency of NETOPS, the signal regiment provides geographical combatant commanders the personnel and tools to collect, transport, process, protect, and disseminate information. The NETOPS and defense

capabilities provided by Signal Soldiers play a critical role in enabling combat successes and prevailing in the information war.

FM 6-02 will provide the tactics and procedures associated with NETOPS. FM 6-02 will also provide the doctrinal foundation for the overall guidance and direction pertaining to mission command of Army communications networks and information services across the range of military operations.

Future Signal Army Techniques Publications will provide greater detail regarding how the Signal Regiment will accomplish its mission. The Army Techniques Publications will expand upon the roles, responsibilities and support discussed within FM 6-02.

Questions, comments, and recommendations related to Signal Doctrine can be provided via e-mail at usarmy.gordon.sigcoe.mbx.gord-fg-doctrine@mail.mil.

ACRONYM QuickScan

DOD - Department of Defense
FM - Field Manual
GIG - Global Information Grid
LWN - LandWarNet
NETOPS - Network Operations

Chief of Signal CHANGE of COMMAND



By Wilson A. Rivera

As the new Chief of Signal took command, the U.S. Army Signal Corps made history and paid tribute to it. Troops used historical semaphore flags to relay commands during the ceremony on 25 July 2012 for outgoing commander, MG Alan R. Lynn, and incoming commander, MG LaWarren V. Patterson. In front of Soldiers, Sailors, Marines, Airmen, and community leaders from around the Central Savannah River Area, MG Patterson became the 36th Chief of Signal.

"What Signaleer wouldn't dream of one day being the next Chief of Signal," MG Patterson said. "It feels exciting, like winning

the lottery."

During the ceremony, the historic semaphore flag signaling system relayed silent commands from the adjutant and commander of the troops to present arms, order arms, and parade rest on Barton Field. Semaphore flags have been used to communicate since 1914. Signaleers stood next to the commander on the battlefield, getting the message though.

LTG David G. Perkins, U.S. Army Combined Arms Center and Fort Leavenworth commanding general, was the officiating officer of the ceremony. LTG Perkins commented on the accomplishments by MG Lynn and the way forward under MG Patterson.

MG Lynn's next command

is with the U.S. Army Network Enterprise Technology Command, in Fort Huachuca, Ariz. MG Patterson makes a short move into the installation commander's quarters after relinquishing command of 7th Signal Command (Theater) headquartered at Fort Gordon.

MG Patterson says he plans above all to take care of all Soldiers and their families, and to make sure the Signal mission is done so that the Army can fight and win the nation's land battles. He added that he quickly wants to get to know the community and be an enhancement to the CSRA.

"This is something I've wanted to do my whole life," he said. "As retired GEN Eric K. Shinseki once said 'The Army is a passion, ...



Photos by Marlene L. Thompson / Multimedia & Visual Information Center

Soldiers from the the Fort Gordon Installation Support Detachment Cannon Salute Battery fire 13 rounds on 25 July 2012 during the change-of-command ceremony for MG LaWarren V. Patterson, incoming U.S. Army Signal Center of Excellence and Fort Gordon commanding general.



(Above) MG LaWarren V. Patterson, U.S. Army Signal Center of Excellence and Fort Gordon commanding general, passes the Signal Corps Regimental colors to CSM Ronald S. Pflieger, regimental command sergeant major, during the ceremony held 25 July 2012 on Barton Field. (Below) MG Patterson and the official party, are “piped aboard” by a cadre of sideboys at the start of the change-of-command ceremony. Fort Gordon has Navy, Air Force and Marine units stationed on the post.

you’ve got to love it,’ I love the Army, only second to my family,” said MG Patterson.

Wilson A Rivera is editor of the Signal Newspaper at Fort Gordon, Ga.

“I will give you my utmost...I shall expect yours.”

MG LaWarren V. Patterson
36th Chief of Signal



Signaleer assumes command of AMC

(Below) GEN Dennis L. Via, Army Materiel Command commanding general, passes the AMC guidon to CSM Ronald T. Riling, AMC command sergeant major, during the AMC change-of-command ceremony, 7 August 2012.

(Right) During his promotion ceremony, GEN Via's sons, Brian (*left*) and Bradley, pin four-star rank on their father. Later in the day, GEN Via assumed command of the Army Materiel Command. GEN Via is the first Signal officer to be promoted to four-star general. AMC's mission is to develop, deliver and sustain materiel to ensure a dominant joint force for the United States and our allies. AMC serves as the focal point in the Army where superior technology, acquisition support, materiel development, logistics and power projection/ sustainment are contracted and integrated to assure current and future readiness.



The U.S. Army Materiel Command is the Army's premier provider of materiel readiness – technology, acquisition support, materiel development, logistics power projection, and sustainment – to the total force, across the spectrum of joint military operations.

OPERATING ON UNCONVENTIONAL TERRAIN

LTC Michael Lanham

The question “How can the Army better plan and execute effective cyber defense?” is too broad. We can craft more effective solutions if we narrow the question. And we can develop approaches that more closely align with traditional military vocabulary and symbology than does our current tendencies to ‘go geek.’

The approach, is to use the military decision making process, augmented with doctrinal Joint and Army graphics, and treat cyber terrain approximately the same as we treat the land and air domains.

Using the mnemonic of mission, enemy, time, terrain, civilians, we’ll ask some clarifying questions, starting with “Better than what?”

How will we know when we are ‘better’ (mission) and if the improvement is enough? What resources (troops, terrain, time, equipment) are avail-

able to become ‘better’? What are the constraints and restraints (mission, civilians, enemy, time, ROE)? Is there a prioritized threats list or defended asset list such as Air Defense Artillery creates/uses? Is the commander willing to conduct economy of force operations in defending one or more cyber positions, routes, or line of communication?

Is defense of the secure internet protocol network, given its cryptographic separation from other networks, one of those economies of force operations? Can our economy of force operation be all or some of the non-secure internet protocol network positions—even though our sustainment (person-

nel, finance, maintenance, and strategic and tactical logistics) warfighting function does most of its work there? How concerned is the commander with threats to morale-oriented use of DoD cyber infrastructure compared to threats exploit such use as an avenue of approach to NIPRNet and shared infrastructure?

Cyber defense planners need to know current threats (enemy, civilians, troops) as well as current friendly situations two-levels-up and one-level-down (troops, commander’s intent). With that knowledge, it’s extremely likely that COA recommendations for the physical and cyber AORs will contain multiple decision and branch points. Examples of decision

points include: whether to isolate (clear cyber fires) units in contact against immediate/high impact cyber threats to other units; whether and how to clear cyber fires for units not in contact against slow-spreading malware; whether to temporarily exempt some mission areas and units (e.g. aeromedevac for combat theaters) from anti-malware directives; whether and how to react to a fast-moving

threat, even with some units in direct fire contact; to whom can the Commander permanently or temporarily delegate such decisions.

There are multitudes of other questions for which we need, at least approximate, answers as well as approximate first and second order effects. Asking for guidance and offering COAs to our commanders is essential—or our commanders will discover they have a set of defenses, on disadvantageous real and/or cyber terrain, that don’t adjust to enemy actions as the commanders envisioned. They’ll also discover

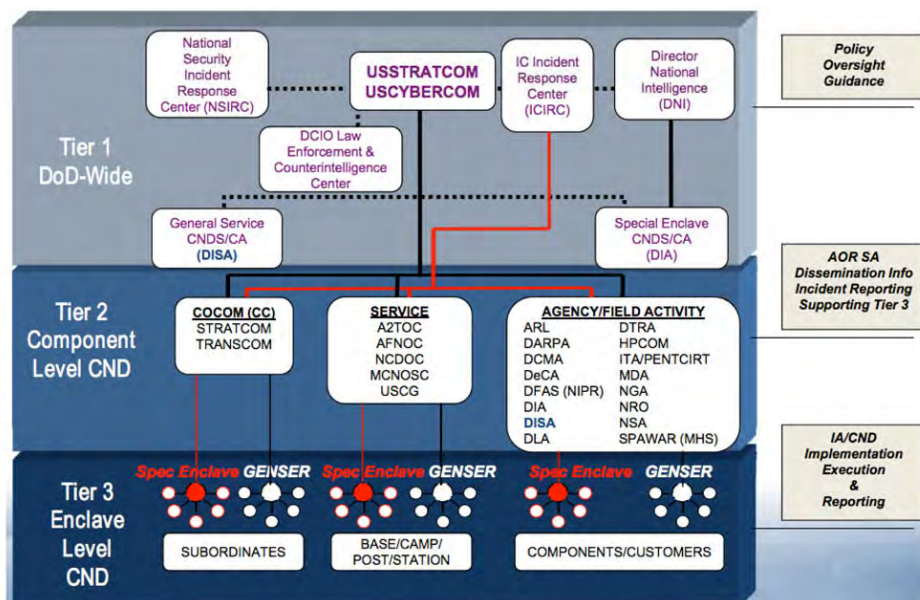


Figure 1 U. S. Cyber Command as the Tier 1 CND-SP

(Continued on page 8)

(Continued from page 7)

that their assumptions about the J/G/S6 just 'getting it done' can leave them reaction choices that don't fit their scheme of maneuver.

The original question of this article implied a requirement to be 'better' than the status quo. How do we know we've sufficiently met that requirement? We can recommend measures of performance and measures of effectiveness. A possible MoP could be, "a 10% reduction in loss of availability of IT systems needed for operations." A possible MoE could be, "an 80% reduction in the number of combat missions that have failed due to loss of IT systems."

With these candidate measures, we've reached a challenge in expectation management. Which 'operations'--tactical combat operations by a platoon conducting an ambush or periodic VTCs between a HQ's forward and main command posts ... the transition between strategic and tactical logistics operations... or the

planning and execution of a tactical resupply mission?

With a vague MoE, to establish a reduction, we have to have some idea of a baseline, or ground truth. Has any COCOM or Army unit determined how many and what types of missions have failed due to a loss of cyber capabilities? Of the many possible MoPs and MoEs, these two derive from the apparent dominance of non-availability and mission failure in the rhetoric of public discourse.

U.S. officials have repeatedly sounded the alarm about our unpreparedness for cyberspace warfare. Public figures routinely refer to the potential for loss-of-life and 'existential threats.' They often speak about the potential for devastating consequences from a large-scale cyber attack. Of note is the lack of reference to documented cases of loss-of-life, destruction of companies, or disruption of public utilities directly attributed to cyber operations. Also missing is reference to large-scale destruc-

tion of civil society in the absence of IT-enabled life. Large-scale power losses in the U.S. Northeast and U.S. Midwest-to-Eastern-seaboard suggest a greater resilience to cyber-less life than the rhetoric acknowledges. India, Estonia, Ukraine, and Georgia appear to reflect the same resilience to cyber-less and cyber-disrupted life in the long term.

The disconnect between demonstrated civil/governmental resilience to natural disaster and rhetorical predictions of cyber catastrophe makes developing and distributing relevant MoE and MoP even more critical for cyber defense planners and commanders.

Army Regulation 10-87 states that "All operational Army forces are assigned to combatant commands." Incorporating this, we can modify the original question to, "can COCOMs and their assigned Army forces plan and conduct cyber defense operations better than the status quo?"

This choice allows us to separate more frequently volatile AORs from the non-operational forces and the supporting institutional base of the Army. It also avoids the interminable debates about the proper division of Service Title X and COCOM Title X responsibilities and authorities. Those debates tend to revolve around perspectives about cyber-personnel and the equipment/networks: Services extend, under their control, their capabilities into Joint and Coalition AORs versus Services provide capabilities under COCOM authority to meet theater Joint and Coalition operational requirements.

A further refinement of the original opening question can be, "Can COCOMs, and their assigned Army forces, plan and conduct cyber defense operations in all phases of operations to ensure continued readiness for and execution of military operations?" This construction

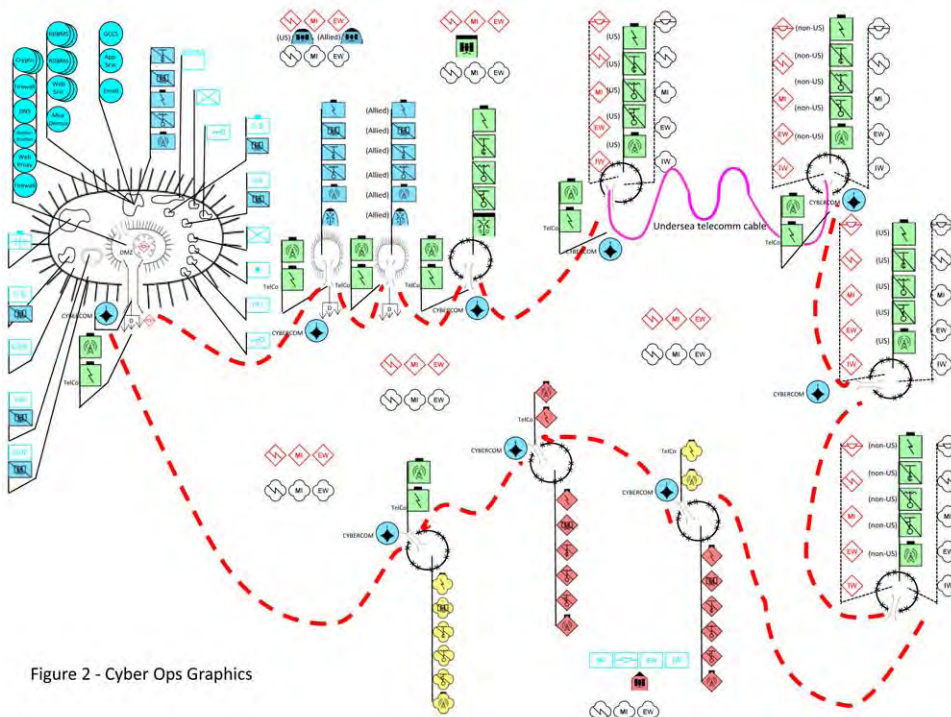


Figure 2 - Cyber Ops Graphics

Figure 2 Operational Graphics Representing a Cyber Operation Battlespace

Figure 1 depicts U.S. Cyber Command as the Tier 1 CND-SP. As of late 2009, no COCOM other than USSTRATCOM had created their own CND-SP, instead hiring DISA as the CND-SP for their headquarters' cyber positions. This and many others decisions have lead to a situation where, unless CND-SP actions crossed into operational channels (e.g. Operation Buckshot Yankee), the COCOMs relied upon the Services to provide CND-SP capabilities to COCOM forces. This creates a de facto line of authority between the Services and COCOM forces that does not otherwise exist in joint doctrine.

Returning to the modified question, a last refinement could be “Can COCOMs and their assigned Army forces plan and conduct a deliberate defense of cyber capabilities in all phases of operations to ensure continued readiness for and execution of military operations?” In short, instead of using the civilian-dominated language of enclaves, intrusion detection systems, and firewalls, use Joint Publication and Field Manual 1-02 language such as sensor, positions, strong points, LOCs, communications zones, deliberate defense, and deliberate operations. Though JP 1-02 defines a deliberate defense as “normally organized when out of contact with the enemy,” our need to create an “extensive fortified zone” clearly applies. The definition of deliberate operation, “An operation in which a commander’s detailed intelligence concerning the situation allows him to develop and coordinate detailed plans, including multiple branches and sequels...” is also clearly applicable.

This construction of the original question will face resistance, as it requires an acknowledgement that many positions of DoD, COCOM, and Army cyber infrastructure are fixed on both physical as well as cyber terrain, requiring a permanent defense. That acknowledgement stands in contrast to the central idea of Army Doctrine Publication 3-0 Unified Land Operations: “seize, retain, and exploit the initiative to gain and maintain a position of relative advantage in sustained land operations to create conditions for favorable conflict resolution.” To seize initiative in permanently defensive situations will place unfamiliar demands on commanders and their staffs.

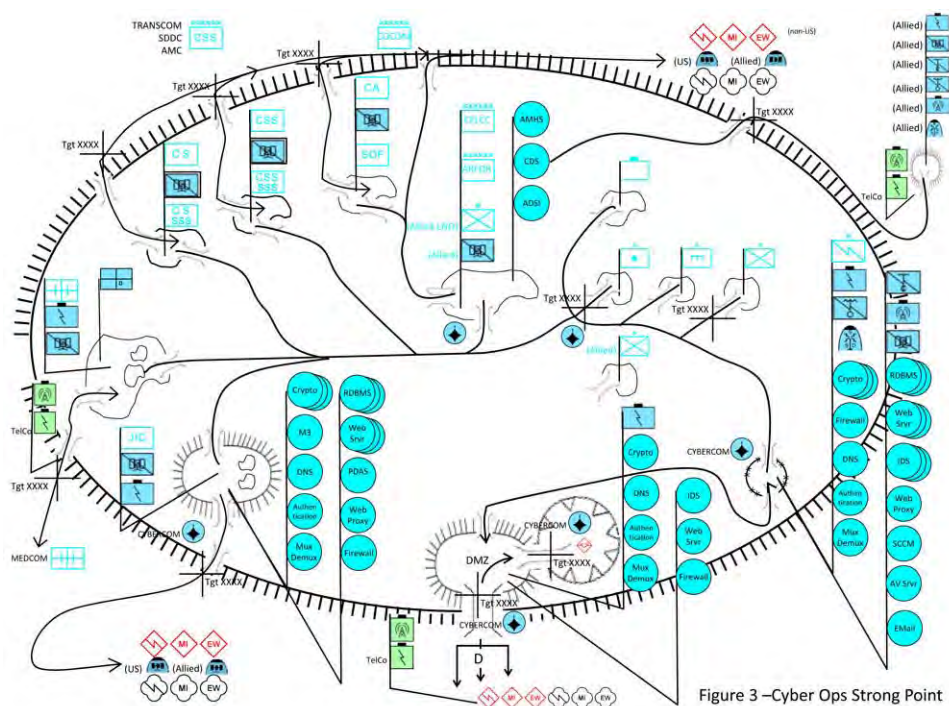


Figure 3 Cyber Strong Points

When planning a deliberate defense, or any operation, our professional military education system teaches Soldiers that the Commander is an essential figure. To help ensure commanders stay involved and interested in cyber defense planning, their subject matter experts should drop the vocabulary of Intel, Cisco, Microsoft, and other ‘geek speak’ and revert to traditional military operations vocabulary.

An example of this reversion is Figure 2. It is a set of operational graphics that represents a cyber operations battle space. Using Military Standard-2525C (with some allowances for different software tools and modifications to cope with the newest addition to war fighting domains), we can communicate a significant volume of relevant data to any commander. The figure uses symbol sets she/he is used and communicates the relationship of units to their cyber positions (and physical positions if placed on a map overlay). Within this strong point there is a gap in the defenses indicated by the bridge icon, with a disruption icon to indicate that cyber forces must disrupt enemy approaches into the strong point. Further, the depicted ASCC commander can see the existence and location of multiple USCYBERCOM sensors throughout the battle space. He can see and communicate to his subordinates that there are multiple enemy approaches into the strong point. The figure also communicates to the various units inside the strong point that they have their own boundaries/demarcations they must defend. The figure also levies a number of implied tasks

(Continued on page 10)

(Continued from page 9)

to the cyber defenders and traditional Signal support units. The graphic shows multiple units with their own generic tactical satellite icons – planners can use modifiers to depict specific capabilities (e.g. CSS-VSAT, JNN. There are template enemy graphics as well (a software limitation prevented use of dashed lines) as well as the intent to isolate enemy sensors

within the DMZ. Importantly, the diagram reveals the dominance of neutral (green) telecommunications companies and telecommunications infrastructures just outside their strong point perimeters. This dominance is true even in Afghanistan and Iraq.

In Figure 3, the cyber strong point diagram puts details to the phrase defense-in-depth. Figure 3 shows an overall protective perimeter, a controlled entry point,

a cyber turning obstacle to route attacks to an isolation area, as well as responsibility for interior perimeters defense. To a maneuver commander, this depiction should start a detailed discussion about likely enemy avenues of approach, primary, alternate, contingency, and emergency positions and cyber actions on contact – all conventional plans even though its non-traditional terrain.

A commander can pre-plot cyber fires that allow her/him to interdict or destroy enemy activity on internal routes between units. There is the visual cue that internal cyber routes need periodic clearance to remain under friendly control. Several units have redundant communications paths through the installation telecommunications facilities as well as their own tactical satellite access. This redundant capability suggests the need for increased security and monitoring at additional ‘holes in the wire’ to avoid weakening the overall strong point.

Like Figure 2, the diagram levies implied tasks on cyber operations units and Soldiers. It is essential to know which cyber capabilities belong to which units. The diagram emphasizes the reliance on neutral telecommunications companies. The diagram also illustrates planning considerations for cyber defenders that are often overlooked: Army provisioning of network access (NIPRNet and SIPRNet) to coalition partner liaison officers and elements; having dedicated routes for shared ADA situation awareness; having MI-owned strong points supporting JWICS; setting up and rehearsing the response to call for cyber-fires on pre-planned targets; setting up an isolation area(s); physical defense of satellite downlink stations, telecommunications and radio relays at the technical control facility; units within the perimeter that are collocated but not otherwise under the command authority of the ASCC (e.g. SDDC, AMC); and

Advantages	Disadvantages
<ul style="list-style-type: none"> •Rapid information sharing via use of standardized JP I-02 and FM 1-02 vocabulary and iconography •Visually combines area defense and point defense coordination of entry/exit points, PACE routes and capabilities, and mutual reliance for security •Within area defense, emphasizes template enemy presence throughout the cyber-LOCs, with implicit requirement to reduce or mitigate the enemy’s presence •Operational requirement to control friendly and enemy cyber-LOCs becomes obvious •Depicts requirement for cyber-coordination between units •CAN planning at appropriate echelons will have better SA of impacts within an AOR •Helps plan and visual enemy cyber attack points, approaches, locations for friendly effects/obstacles (e.g. canalize, turn, disrupt, isolate) 	<ul style="list-style-type: none"> •Map/graphics reading and interpretation is a perishable skill •Not all Soldiers from all warfighting functions are comfortable with MIL-STD-2525C •Threat type differentiation (e.g. nation state sensor vs. cyber criminal vs. teenager in Paris/Des Moines) requires icon modifiers •MIL-STD-2525C has no way of reflecting equipment/capability dependencies except through co-location •Map/graphics overlay requires maintenance effort
<p>If control of cyber LOCs is not feasible due to neutrality, then</p> <ul style="list-style-type: none"> •Guard the friendly entrances and exits that touch those LOCs •Pre-plan targets on the LOCs with permission from higher •Gain clarity on neutrality of cyber-LOC providers 	<ul style="list-style-type: none"> •Cyber Intel applicable to AOR and units becomes yet another product unit J/G/S2 has to find/generate •Geo-plotting every device may have a low ROI for many units/locations
<ul style="list-style-type: none"> •React to enemy cyber contact may become faster •SA of units/capabilities not using Signal assets •SA of units/capabilities using Signal assets •Combined with capabilities such as host based security services (HBSS), should increase per IT SA as well as per unit cyber SA •Geo-plotting makes command responsibility immediately clear •Helps pre-plan cyber fires for units within an AOR and for units outside the AOR •Rehearsals of target/fires increase confidence in response time and probability of gaining effects •Should help in clearing offensive/defensive fires across unit boundaries 	<ul style="list-style-type: none"> •Commanders at wrong echelons may perceive greater latitude for offensive and defensive cyber operations than exists •Requires targeting process participants to gain familiarity with •cyber targeting, cyber effects, cyber BDA (e.g. artillery destroy !=cyber destroy; cyber deny!=engineer deny) •processes established for cyber fires by USCYBERCOM and CYBER-JIATF •Will likely cause an increase in templating and requesting cyber fires for defense and offense •USCYBERCOM may not be capable of supporting quantity of requested fires •USCYBERCOM may reprioritize local targets in favor of strategic targets of interest
<p>Unit boundaries can align with IA demarcation points for systems and enclaves, e.g. bridges in/out of theater enclaves, JTF enclaves division or brigade enclaves.</p>	<p>Clean alignment of physical boundaries and demarcations may not be feasible. DISA Tier 0 network equipment is frequently co-located with P/C/S TCF</p>

Advantages and Disadvantages of using JP 1-02 vocabulary and concepts

the heavy reliance by CS and CSS units on non-Signal-provided capabilities.

I have not included a figure that incorporates maneuver graphics and AOR boundaries but they could easily help reduce misplaced perceptions of responsibility while bringing home to units their actual contributions to cyber defense operations. Every COCOM has a number of physical and cyber strong points within their geographical or functional AOR, connected by ground, air, and cyber LOCs. Those cyber-LOCs enter and exit their AOR at physical points as well as logical points — those points can become coordination points/icons, targets, and sensor emplacement points. Plotting units and capabilities physically and logically also supports more rapid clearing of defensive cyber fires as envisioned in what USCYBERCOM calls 'active defense,' and reduces the likelihood of unintended consequences.

Figures 2 and 3, and the figure described above, communicate a complex but traditional military operation, on non-traditional terrain. This approach supports Commanders and staffs ability to think about the cyber domain in approximately the same terms as their air and land domains. Commanders will learn where pre-planned defensive cyber fires exist, their probable operational impact when fired, and can plan compensation measures. Through awareness of dependence on civilian infrastructure, they can build and rehearse PACE plans for communicating to and with higher and lower units. There are a multitude of potential advantages listed in Table I, and for balance's sake, predictable disadvantages as well. Though I make no claim the list is comprehensive, it should at least provoke reflection on the collective wisdom of abandoning a common lexicon and adopting a 'new' one — for whatever the reasons.

Table I Advantages and Disadvantages of using JP 1-02 and FM 1-02 vocabulary and concepts

There is a strong underlying message in my assertion that cyber defense is a traditional military operation: decentralized COCOM operations, as inefficient and chaotic as they are, should remain the order of the day. Defending a set of inter-connected strong points in a region is not a military operation that the COCOMs or the Army trains to conduct via centralized execution. Instead they nest task and purpose to support the intent of centralized planning without the inflexible application of centralized approval. This nesting allows for dealing with the surprises of 'reality' vs. 'the plan.' The nesting allows COCOM commanders to assess and balance risks and operations as close to their operations as feasible while allowing other COCOMs and potentially effected commands options to reduce their own exposures to those risks. Indeed, if the job of balancing regional and global or Service perspectives is centralized, its more likely than not that the needs of the many will always outweigh the needs of the few — to the

detriment of the minority conducting highly volatile operations. Unfortunately, there is a multitude of past and current trends, policies, personalities and efforts within the Joint arena and the Army to make defense of cyber strong points and LOCs centrally executed. This is in contradiction to our national willingness to decentralize most combat operations, clearly a matter of life-and-death. Historians often cite that willingness, indeed the apparently ingrained inability to do centralized execution, as one of our greatest military strengths. Our growing unwillingness to resource and execute decentralized cyberspace operations is disconcerting. The efforts to move toward centralized execution are, in actuality, grand experiments, with as little proof of future success as this article has presented. I submit to you that the burden of proof when advocating wholesale change is on the advocates of that change. I've not seen evidence in classified or unclassified realms that convinces me of the added value of creating unique-to-cyber processes and vocabulary. Nor have I seen evidence of the value of abandoning graphical depictions used so successfully in the other warfighting domains.

I have been exposed to two schools of thought for involvement of operational force commanders in cyber defense planning and execution. Paraphrasing, one such school is that cyberspace is far too important and complex to leave to maneuver commanders. The other school is that cyber defense will not succeed without commanders. I clearly subscribe to the second school despite copious evidence of disinterested commanders and staff leading to poor cyber outcomes. I've also seen even more evidence that excluding maneuver commanders from cyber defense and planning leads to, predictably, worse outcomes than had those commanders been involved.

I submit to the readers that we, formally the Army's cyber-SMEs, must use the language of our maneuver commanders if we are to succeed in engaging their interests. I have proposed use of a traditional planning method and traditional doctrinal vocabulary (with minor updates) for planning and executing cyber defense for operational forces. I have proposed that staying in that realm of vocabulary and iconography is more likely to retain the interest, understanding, and resource commitment of commanders than by 'going geek' on them.

I have offered no proof that this approach to planning will actually make COCOM and assigned Army forces better at cyber defense. Indeed, the absence of proof in cyber defense policy, advocacy, efficacy, and efficiency discussions is endemic within the DoD — we frequently substitute passion and hyperbole for evidence, use measurable quantities (e.g. costs) as proxies for inherently qualitative assessments, and break into

(Continued on page 12)

advocacy camps convinced of our own righteousness. We use short-duration joint and warfighting experiments that don't allow long-term, significant, and effective disruption of cyber capabilities in the actual experimental networks. We conduct C3I experiments that allow disruption, with insufficient operational impact assessments by commanders — I've attended simulations where a 'glitch' led the players to go to lunch, instead of continuing the experiment. I've seen decisions to implement PACE plans for cyber capabilities be furiously argued as the staff and the commanders weigh the immediate pain of rehearsal with the promise of being more resilient to non-specific threats of denial or degradation. Anecdotally, these examples are not unique, though I have no sense of their relative frequency. It's my assessment that we have a Joint and Service shortfall in our ability to conduct long-term cyber experiments as well as organization redesign in reaction to cyber events experiments — how to address that shortfall is an article for another day, though I strongly suspect agent-based socio-cultural simu-

lations and dynamic socio-network analysis is a key enabler we inadequately use.

There are at least five conclusions we can draw from this discussion: 1) operational force commanders are essential for operational force cyber defense; 2) we can plan and execute cyber defense by considering the mission a traditional deliberate operation on non-traditional terrain; 3) this approach will be uncomfortable to portions of the CND communities; 4) advocates for centralizing cyber defense have the burden of proof to justify violating operational norms; and, finally, 5) simulation or proof of future success is beyond our current institutional ability.

***LTC Michael Lanham, IN,** is a FA53 in Advanced Civil Schooling pursuing a PhD in a field of Computer Science. He has served as a Theater IA Program Manager at ARCENT, a CNO plans officer at ARFORCYBER and JFCC-NW and deputy Chief Information Officer at JFCC-IMD. He has bachelor's degrees in Computer Science and Computer Engineering and a master's degree in Computer Science.*

Join the Discussion
<https://signallink.army.mil>

ACRONYM QuickScan

ADA – Air Defense Artillery
ADP – Army Doctrine Publication
ADSI – Air Defense Artillery System Interface
AMHS/M3 – Automated Message Handling System
AOR – Area of Responsibility
ASA – Assistant Secretary of the Army
CC – Combatant Command
CC/S/A/FA – Combatant Command, Service, Agency, Field Activity
COMMZ – Communications Zone
CPN – Command Post Node
CND-SP – Computer Network Defense Service Provider
COCOM – Combatant Command
CS – Combat Support
CSS – Combat Service Support
DEMUX – De-multiplexor
DEPOD – Deployment Order
DISA – Defense Information Systems Agency
DHS – Department of Homeland Security
DMZ – Demilitarized Zone
DNS – Domain Name Service
FA – Field Activity
FOB – Forward Operating Base
FCC – Functional Combatant

Command
GCC – Geographic Combatant Command
HBSS – Host Based Security Services
HQDA – Headquarters, Department of the Army
IA – Information Assurance
IP – Internet Protocol
ISEC – Information Systems Engineering Command
IT – Information Technology
NLT – No later than
P/C/S – Post / Camp / Station
JIATF – Joint Inter-Agency Task Force
JNN – Joint Network Node
JP – Joint Publication
JPG – Joint Planning Group
JS – Joint Staff
JTF – Joint Task Force
JWICS – Joint Worldwide Intelligence Communications System
LOC – Line of Communication
LNO – Liaison Officer
MDMP – Military Decision Making Process
METT-C – mission, enemy, time, terrain, civilians
MIL-STD – Military Standard
MoE – Measure of Effectiveness

MoP – Measure of Performance
MUX – Multiplexor
NCO – Non-commission Officer
NIPRNet – Non-secure Internet Protocol Network
NGB – National Guard Bureau
OBV – Operation Buckshot Yankee
OPCON – Operational Control
PACE – Primary, Alternate, Contingency, and Emergency
PME – Professional Military Education
ROI – Return on Investment
SA – Situation Awareness
SECDEF – Secretary of Defense
SIPRNet – Secure Internet Protocol Network
SME – Subject Matter Expert
TACON – Tactical Control
TCF – Telecommunications Facility / Technical Control Facility
TelCo – Telecommunications Company
TTP – Tactics, Techniques, and Procedures
USSTRATCOM – U.S. Strategic Command
USCYBERCOM – U.S. Cyber Command
VSAT – Very Small Aperture Terminal

NetOps, here we come!

Facing some hard questions



By CW5 Todd M. Boudreau

If your most savvy adversary is currently using your highways and byways to transport goods, they are stealing from you. Although they may possess the ability to disrupt your motorways and/or destroy your roads, to do so would negatively affect their own operations.

However, if there was a shift that caused the adversary to value stopping our use of the roadways more than their use of them to transport stolen goods, would we be prepared to defend them... every one of them?

So what does a conversation that may be best suited for Homeland Defense have to do with cyber defense? Change the environment and the scenario remains constant. Open source intelligence acknowledges that our communications platforms and transport systems (i.e., data highways) are under constant attack through probes and malware every day. Much of what we see is cannon fodder. However, unmitigated it drastically increases the noise floor making it possible for a skilled adversary to surreptitiously enter our networks, gain a foothold into our information systems, and begin Computer Network Exploitation actions such as exfiltrating data.

If, however, there is a change in relations with said adversary due to a political decision or kinetic contest somewhere in the world, said adversary could easily shift from CNE operations to a Computer Network Attack posture. With the criticality of our technology systems to our combat operations, are we ready to operate while an adversary attempts to manipulate data and/or to disrupt the operations of, deny our uninterrupted access to, and/or destroy our information systems?

Few today would argue that defending our communications systems and the critical information within them is more than a full-time job; but not so many understand that everyone has a level of responsibility.

Just as a reminder, take a moment to remember (or imagine for those who did not live the days of Mobile Subscriber Equipment and Tri-Service Tactical; MSE and TRI-TAC respectively, the magni-

tude of barriers our opponents faced in the days of MSE and TRI-TAC to gain entrance into our military networks, just under the perspective of equipment, architecture, and investment. The equipment used under the MSE and TRI-TAC programs was proprietary; Commercial-off-the-Shelf equipment had not yet been popularized in tactical transport services.

The architecture, even though it included meshed networks, was based off a circuit switched paradigm which afforded some level of Low-Probability-of-Interception. So, there was a substantial investment required to attack such a communications system.

Those with intent to attack our networks did not necessarily pose a threat since they did not also possess knowledge of vulnerabilities and the capability to exploit said vulnerabilities. As the equipment was mostly proprietary, an adversary would need to obtain and reverse engineer our equipment, and then identify vulnerabilities; then such a foe would need to create or exploit the opportunity to intercept a circuit switched, encrypted, timed trunk dependant communications link – all huge barriers in themselves.

Today, however, over ninety-percent of our military communications infrastructure, platforms, and programs are COTS; software and equipment available to anyone. Our current TCP/IP architecture was developed for transparency, interoperability, and technology insertion; not necessarily with security in mind. As vulnerabilities are identified they are oftentimes posted in the open for all to see. Capability sets to attack and exploit such vulnerabilities are easily obtainable.

So the substantial investment required to attack has been significantly reduced, creating a converse and exponentially increased investment required to defend; the Federal Government reportedly spent \$12B in IT Security in 2010; 15% of its total IT spending.

Those with intent to harm our military communications networks and to exploit and/or

(Continued on page 14)

How well are we prepared to face a peer, or even a near-peer adversary in our cyberspace?

(Continued from page 13)

manipulate critical information merely need to know where to look to find a virtual cornucopia of attack capabilities. With \$50k, anyone with inclination and desire can hire a botnet and launch a distributed denial-of service attack; similar to those that struck South Korea, Georgia, Estonia, and yes, even segments and portions of the United States.

While in the past, the technical complexity required of the attack capability was to our advantage, today various aspects of technology, to include its availability, have added to the necessary technical complexity of the defense capability. For example, the average low-tech, yet often effective, attack toolset is in the order of hundreds of lines of code, whereas the average defense toolset is in the order of millions.

What is needed is the ability to invoke a machine-on-machine response in order to counter attacks made at network-speed. And while we have made great strides toward that end, a myriad of obstacles have yet to be breached. To that end, we need everyone involved in the defense of our communications networks and systems. I could go on and talk about the need for the common user to understand cyberspace as an operational domain and to be able to make parallel connections such as viewing emails from unknown recipients as possible unexploded ordinance or cyber incoming. I could also spend time talking about how important it is for our senior leaders to understand the imminence of the threat and consciously measure the importance of our essential cyber terrain. However, instead I would like to challenge us, Signaleers, Cyber Warriors, those of us interested enough to read the articles in this *Army Communicator*.

How well are we prepared to face a peer, or even a near-peer adversary in our cyberspace? Beyond establishing an up-armored cyber defensive posture, beyond ensuring all policies and governance has been followed, beyond ensuring all systems are patched and up-to-date, are we prepared to build, manage, and shape our cyberspace to ensure we maintain the advantage when our adversaries have entered and are performing disrupt, deny, destroy operations? When our networks and networked systems, installed, operated, and maintained by us are no longer uncontested operational

space, are we ready, prepared, and able to ensure uninterrupted Mission Command Essential Capabilities?

While we are shaping our cyber workforce to include expert defenders who are able to understand the adversaries tactics, techniques, and procedures, response actions, or better yet preemptive response actions within our own LandWarNet requires experts in transport and complex Mission Command systems as well. As I asked in my opening comments, although we have a NetOps construct, are we really conducting, or even able to conduct true Network Operations? Are our experts in transport and routing able to make changes beyond reactive optimizations based on bandwidth demands? Are our experts in establishing data services able to adapt beyond a static model of Mission Command service expectations and out maneuver an aggressive adversary in a contested battle-space? Are we collectively trained, tested, and prepared to conduct NetOps?

Armed with knowledge, actionable intelligence, and a host of tools (both specifically specialized as well as converged such as the Defense Information Systems Agency's Host-Based Security System) our expert cyber defenders hunt for potential adversarial activity used to prepare for CNE and/or CNA activity in order to catch and posture for response actions before any damaging activities can be accomplished. Once anomalous activity is identified and categorized as adversarial, pre-coordinated actions in accordance with an established playbook are initiated. In many cases, such actions will include immediate preemptive transport routing modifications as well as data screening, filtering, and transition to alternate servers.

The cry of this article is for an understood, acknowledged, collectively trained NetOps posture enabling us to make appropriate adaptations to our operational portion of cyberspace in the midst of a peer or near-peer adversary's attempt to deny us freedom of movement, disruption of critical services, and/or manipulation of critical information. Are we there yet? If not, either by design or by necessity...NetOps, here we come.

CW5 Todd M. Boudreau is the U. S. Army Signal Regiment Chief Warrant Officer.

Studying offensive computing is essential

MAJ T.J. O'Connor, CPT Ryan Hand, CW3 Matt McDougall

An effective defense for successfully repelling threats to our networks must include a knowledgeable offense.

Combating the threats to our military systems is one of the most critical roles of the Signal Regiment. In the last six years, the number of reported cyber attacks has grown by 650 percent. Our adversaries' capabilities are exponentially multiplying attacks on networks.

As we Army communicators charge forward into this challenging domain of warfare, we must ask relevant questions. One of the hard questions to be asked and answered is "Do our Signaleers have an adequate basic understanding of the elementary tactics, techniques, and procedures in this domain of warfare?"

For our officer professional development program, we began exploring some of the concepts involved in offensive computing, because we really don't know what we don't know about our adversaries' tactics.

Over the last 12 months, the Signal officers in our unit began taking the same classes as attackers, studying how our adversaries operate, analyzing the operational successes of organizations like Anonymous and learning to hack.

Studying concepts like penetration testing, exploit development, wireless exploitation and forensic recovery, we learned to attack exactly like the adversary. We traveled to compete and win hacker competitions, remotely attacked toy unmanned aerial vehicles during officer professional development lunches, and wrote



The best defense begins with a strong offense.

and developed open-source attack tools. Twelve months of this professional development has brought us to some interesting understandings that we would like to share, in the hope that as a Regiment we can learn to defend this domain of warfare better.

Tried-and-True Means Tried and Exploited

All too often military experiences teach us to only apply tried and tested concepts in warfare. Consider when the Marines sought a viable rotor-wing aircraft to rapidly insert small teams into Afghanistan. Marine Detachment 367 selected the UH-1Y Huey, an updated version of a Vietnam-proven close-air support helicopter. With minor modifications to the weapons systems, the Marines built an aircraft capable of close-air support, small-team insertion and extraction, and casualty evacuation.

Building upon what had already been proven during Vietnam; the Marines re-launched an almost retired air platform in less than two years. Consider this against the lengthy and tragic process of making the Marine Osprey a viable air platform, and you can begin to understand why military planners think this way.

However, these concepts do not translate to cyber. Let's examine why. After brief study as attackers we realized that defending Windows XP is nearly impossible. There is simply no way to patch a decade-old operating system successfully. Incremental versions of Microsoft's flagship operating system have included security mechanisms such as a randomized address space, prevention from overwriting exception handling, and a non-executable stack. These seem

(Continued on page 16)

like foreign concepts to a defender-only versed individual. However, to an attacker it means the degree of difficulty in writing an exploit program goes from requiring one high-school computer science class to a PhD in computer science.

Failure to understand this concept is not only a military-oriented problem. In April 2011, RSA confirmed that they had been compromised by a novel exploit for Microsoft Excel. The exploit infected several systems in the company, ultimately leading to the theft of the source code for their proprietary SecureID product. Later that summer, the same attackers used the proprietary code to attack RSA's customers, Lockheed-Martin and Northrop Grumman. A November 2011 research report concluded that the exploit would have failed if RSA had used a more modern version of the operating system that enabled hardware DEP by default. It is difficult to fully comprehend the concept that we should be using bleeding-edge operating systems instead of stable proven systems. It is a concept you can only truly understand when you learn to write your first exploit, which leads us to a second point: you must learn to write an exploit program before you ever learn to defend.

No Basis for Defense Without Attack

All too often in cyberspace we try to separate the concepts of attack and defense. Because of military authorities, clearances, and capabilities, we have separated the roles of each. For the most part, the Signal Regiment has taken the role of the Army's network enterprise defenders; but how can you truly consider yourself a defender without ever having attacked a system?

To understand this concept, consider the role of a young infantryman. He does not consider himself an offensive or defensive infantryman. He understands that the battle lines will shift over time and he is not fixed on one specific role. He may spend one day on the offensive, pursuing the enemy deep into his territory. The following day, he may be asked to guard a resupply convoy from the same enemy. As an infantryman, he teaches, mentors and coaches his subordinates on tactical movement and weapons systems, studying how either side of the battle may employ them.

Yet Army leaders and planners are largely drawing battle lines in cyberspace. This can only help to create the weakest defenders possible. How does an enterprise defender know how to look for

indicators of a compromise if that person has never compromised a system? In 2006, the Pentagon disclosed hostile cyber units attacked our NIPRNET and downloaded up to 20 TB of data. The attackers used a technique of passing the hash from internal systems to grant unified access to co-located and co-managed systems. Only once finding sensitive data, the attackers compressed that data into compressed archives and pushed it outside our network to foreign file transfer protocol servers.

Twenty TBs leaving our networks is a needle in a haystack for an ignorant defender to classify as malicious, but to a trained attacker that needle is as obvious as the Empire State Building. Compressing data and pushing it to FTP servers to reduce a signature is a junior varsity attacker move. The fact that the same data went to foreign FTP servers would have been spotted by anyone who has ever attacked a system. Unrolling those clues and tying multiple remote process execution commands to them would confirm the attack. Like the infantryman who pauses to examine and disable a trip wire before assaulting an enemy's base, we must understand that our role in cyberspace is not clearly offensive or defensive. When we understand how to attack, we begin to see our defense surface much more clearly.

We Are Only Defending the Visible Attack Surface

Consider the defenses emplaced in your organization for cyber defense. How much did you spend ensuring that cabling was shielded from electro-magnetic emissions? Anyone who has ever built an Army network knows the immense struggle to accredit a facility to process SIPRNET traffic. We emplace a protective distributed system to deter and/or make difficult physical access to the communication lines carrying national security information. We ensure there are approved electronic locks on our network closets. We only procure equipment through reputable U.S.-only based vendors. Annually, organizations spend millions on these defenses. Why? These defenses are critical to our overall defense posture. However, we have a habit of only placing these defenses where we can physically see them. Looking at a locked comms closet with a biometric authentication, we feel like we are making adequate and complete defense. Defending only the physical visible attack surface can ultimately lead to failure. But we'd argue it is a mindset that is prevalent in today's Army. All too

often enterprise defenders think systems are safe if they are physically secured and patched with current updates and anti-virus programs. This is untrue.

Early in the Spring of 2012 we participated in a hacker tournament where we had to gain access to several unauthorized systems in a virtual environment. Lacking physical access, we had to gain system level privileges to a fully patched computer on a virtual enterprise network. Sounds difficult, right? No physical access, system fully patched, anti-virus program running. Should be good, right? No. Within minutes, we found a separate client workstation and sent the user a spam e-mail with a link to an unsigned malicious java applet.

The user clicked the link and ran the applet, granting us full permissions to that machine. At this point, we noticed the machine had an enabled local administrator account. Win! These happen to be the same administrator credentials necessary to log on to our ultimate target. Within minutes, we gained access to a fully patched, well-defended machine.

The attack space is clearly visible to an attacker. They attack things like unpatched remote services, client-side application vulnerabilities, weak credentials, and expose trust relationships. Most network defenders are pretty good about patching systems. However, a defender-only-versed individual fails to see the full defense space, such as ensuring they disable local administrator credentials. An attacker knows this, though, because the password and account policies are one of the first things he or she will examine after initially com-



prising a target. Let's examine another scenario where a weak password can trump even the best theoretical defense.

Implementation Trumps Theory

Most Army Signaleers are familiar with the Federal Information Process Standards Publications. Specifically, FIPS 140-2 contains some guidelines on purchasing IT products that contain cryptographic modules. For example, when purchasing a wireless access point that contains encryption, you must ensure that it complies with FIPS 140-2. Knowing that a body such as NIST has validated the cryptographic algorithms on a device can give an enterprise defender some level of comfort. However, again, it only serves as a false level of

comfort for someone who does not understand the attack surface.

Recently, we asked a colleague to set up a secure wireless access point. After examining all his available options, he chose some sound security-related settings on the access point. He placed the wireless access point in hidden mode (ensuring the access point did not broadcast its network name), enabled MAC restriction (ensuring only specific MAC addresses could connect to the access point), and finally chose the WPA2 handshake-authentication with AES (ensuring that the traffic was prevented from eavesdropping or replay attacks). Outstanding! Our colleague configured the access point in a secure manner as best he understood it.

(Continued on page 18)

(Continued from page 17)

Next, our team attempted to gain access to the access point. We began by sniffing wireless traffic and saw the unencrypted management frames between the access point and our colleague's computer. In an option field of the traffic, we saw the hidden name of the access point. Next, we changed the MAC address of our machine to that of our colleague's computer. With the address changed, we forged a deauthentication packet, severing the original connection. We then watched and captured the WPA2 handshake as our client attempted to reconnect. Running the WPA2 handshake through a brute-force cracker, we noticed the colleague had used a dictionary word for the password. Our colleague was stunned to realize that the password played any role in the overall security of the access point.

While we praised our colleague for knowing all the available options for security, we equally chastised him for failing to choose a secure password. He immediately changed the password to a complex password. Noticing that our colleague had left the default network name as Linksys, we then attacked the complex password using password rainbow tables. Again, our colleague was surprised to realize that the network name played any part in the exchange of the symmetric key for the network. Not surprisingly, he had never attacked a wireless access point before.

There is No Silver Bullet for Defense

So, moving forward, you may ask: What tool should I be using? What can I do to defend my systems? Arguably, we have very good tools for locking down enterprise networks and emplacing host-based controls. However, a good attacker will find a way around them. A decent rootkit can hook the Windows API calls, essentially hiding itself from an antivirus program that scans the file system. Specially crafted fragmented packets can be used in a covert method to evade network capture and network-based intrusion detection systems. In the case of the recent Flame attack, digital signatures can be spoofed to impersonate legitimate software vendors. A layered defense is good – not placing all our eggs in one basket and using multiple network and host-based technical controls is a good strategy.

Continuous education is the most powerful tool we have. Yet, at every impasse, we have noticed individuals arguing for control – “this should be a 255S function,” “only the 53 should be qualified as IAM Level 1,” “a 25 series officer could never understand the complexity of a cyber attack;

he should be a manager.”

There is room for everyone in this domain of warfare. Single ownership of the problem will ultimately lead to failure. Right now, all of our Signal Soldiers need continuous and deliberate education in the domain of cyber war. It must be woven into every aspect of every professional course, training, and exercise. Cyber should closely mirror our Safety and Risk-Reduction programs. Similar to a young platoon leader filling out a risk-assessment card before conducting a rifle range, a young Signaleer should be forced to consider the cyber implications of standing up a new Web server for his unit. Only after repeated, deliberate efforts to learn more about this domain of warfare can we begin to start formalizing solid enterprise defenses against our adversaries.

MAJ T. J. O'Connor is a 25A Signal Officer at the 10th Special Forces Group (Airborne). Prior to serving in his current assignment, TJ taught computer exploitation at the U.S. Military Academy and deployed to Afghanistan and the global war on terror with the 7th Special Forces Group.

CPT Ryan Hand is a FA 53 Systems Automations Officer at the 10th Special Forces Group (Airborne). Prior to serving in his current assignment, Ryan deployed to Iraq for fifteen months with the 63rd Signal Battalion.

CW3 Matt McDougall is a 255A Information Services Technician with the 10th Special Forces Group (Airborne). His previous assignments include the 75th Ranger Regiment and the Joint Communications Unit.



A combined arms approach to defending Army networks

By Russell Fenton

In the face of new cyberspace challenges, we must adopt new ways of defending our networks.

If change cannot be enacted, we will find ourselves mired on the bitter trail of defeated militaries that failed to adapt to changing environments at the time and pace necessary.

We can hear faint rumblings and see the cracks in the walls of our network security. The defenses in confidentiality, integrity, and availability of the information modified, exchanged, and stored by Army networks and information systems is under continuous attack. The incident related to Operation Buckshot Yankee was only one “known” out of hundreds or thousands of “unknowns”; and in the end, terabytes (maybe even petabytes) of data are exfiltrated from Army networks on a yearly basis.

Now that we are fully aware of the continuous threats and some losses of security in cyberspace, we must use this opportunity to develop and gain support for a different approach to defending our networks against a myriad of threats.

Cyberspace is defined as “a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.” Given the inclusion of the terms “information technology infrastructures” and

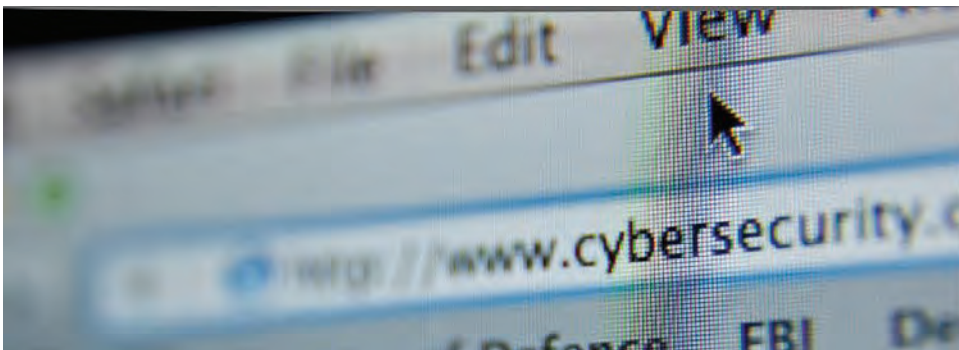
“telecommunications networks” within the cyberspace definition, along with the fact that JP 6-0 (Joint Communication Systems) states “The GIG operates, through cyberspace, as a globally interconnected, end-to-end, interoperable network-of-networks...,” there should exist no doubt that Army networks are the land forces’ application of the cyberspace domain.

As it has for more than a decade, the Army depends on cyberspace [the LandWarNet] to function and create the necessary effects to gain an information advantage over adversaries of the U.S. It is difficult to overstate this reliance. Commanders and leaders at all echelons, whether CONUS or OCONUS, have come to rely on cyberspace to collaborate, gain situational awareness, plan, and conduct mission command at net speed through the full range of military operations. The Department of Defense has recognized this reliance on cyberspace; and subsequently in July 2011, it published a strategy that directs the services to treat cyberspace as an operational domain (as relevant a domain as land, sea, air, and space) to organize, train, and equip so they can take full advantage its potential.

No doubt our adversaries have recognized the Army’s ever-growing dependence on this new domain. Realizing they cannot match the Army force-on-force, nation states and terrorist groups alike are aggressively building capacity to fight us in the virtual realm. This fact foretells a future in which no other aspect of the Army will experience the reality

of persistent conflict more than the LandWarNet. It additionally leads to cyberspace becoming a distinct dimension for warfare in its own right. The warfighters and leaders of the U.S. Army will gain a significant advantage if it can defend the LandWarNet against internal and external threats. But to win that fight, Army leaders must implement a new operational approach that echoes proven land domain concepts in an abstract cyber battle space.

(Continued on page 20)



Cyberspace is a domain critical to mission command and daily operation. Defending cyberspace requires the same combined arms approach that has been successfully used in other aspects of military and domestic operations.

The success of American warfighters in the land domain has much to do with our ability to apply elements of combat power at the time and place of our choosing. The application of combat power requires a combined arms approach that integrates complementary, yet uniquely different, capabilities so that counteracting one makes the enemy vulnerable to another. ADP 3-0 provides an example of this approach when describing how commanders use artillery to suppress an enemy bunker complex, which then enables an infantry unit to close with and destroy the enemy.

Effectively defending the LandWarNet requires that Army warfighters expand our notion of where combined arms must be conducted. In the past, Army leaders viewed the LandWarNet as just an enabler to more efficiently meet information requirements. But combat power needs to be applied in cyberspace just as much as through it. Complementary, yet uniquely different, cyber capabilities across network build, operate, defend, exploit, and attack functions must be integrated in order to find, fix, and finish threats and vulnerabilities inside and outside the network. This does not mean that Army warfighters should do away with the primary objective of fighting and winning in the land domain (successfully defending in cyberspace must lead to a physical outcome). Instead, Army warfighters should recognize the fact that commanders have to leverage the appropriate capabilities as part of a combined arms approach in cyberspace similar to the more established paradigm.

Traditionally, commanders look to Signal elements for the installation, operation, maintenance, and defense of the organization's network. The availability of the network, along with the confidentiality and integrity of the information riding it, are assumed. Vulnerability alerts and network related tasking orders circumvent operations channels and are pushed down through more technical channels. Information about current threat tactics, techniques, and procedures which can be used to proactively implement appropriate countermeasures has been difficult to receive. The result of this has been reduced situational awareness, no unity of effort, and networks that have seen their fair share of exploits.

The idea of a combined arms approach to defend the network establishes a working environment which enables the coordination, integration, and synchronization between the operational processes performed in the current operations, future operations, and plans under an operations section – who disseminate and oversee the execution of the commander's priorities – with the unique network

operate and defensive capabilities provided by the Signal element, and the specialized intelligence, surveillance, and reconnaissance support and specific offensive cyberspace reach-back capabilities provided by the Intelligence community. All this enhanced by other information related capabilities such as inform and influence activities and even knowledge management. Similar to the combined arms example in ADP 3-0 that described the mutually supporting efforts of Field Artillery and Infantry, an example of combined arms in cyberspace would be the use of Signal-related capabilities to disrupt or redirect malicious activity away from critical net-enabled mission command systems, which then allows an Intelligence-related Cryptological Support Element to close with and destroy the enemy's cyberspace capabilities. Expanding network defense operations from the friendly to adversary box increases the situational awareness and unity of effort the Army lacks, and creates an economy of force that ensures commanders can concentrate network defenders when and where necessary.

For more than a year now, leaders in the Army Cyber Command Army Cyberspace Operations Integration Center at Fort Belvoir, Va. have been utilizing a combined arms approach to defend the LandWarNet at the strategic-level. Yet, a recent article by members of the U.S. Army Mission Command Center of Excellence at Fort Leavenworth, Kan. highlighted that to some degree, a combined arms approach is already taking shape at the operational and tactical-level as well. The soon-to-be-published revisions to Field Manual 3-36 Electronic Warfare in Operations will task the commander's EW element to expand and use the EW working group to facilitate the integration of what Army leaders call Cyber Electromagnetic Activities. The overarching objective of CEMA is to gain an advantage, protect the advantage, and place the adversary at a disadvantage in a congested and contested cyberspace and electromagnetic spectrum. However, the solution is intended only as a bridge until the Army develops a more appropriate means to achieve this. Army Cyber Command leaders and the MCCoE, supported by leaders from the Signal Center of Excellence and Intelligence Center of Excellence, amongst others, are working the Army's effort to determine how best to accomplish CEMA integration for the long term.

Current plans envision CEMA integrated within the operations process via the Cyber-Electromagnetic Working Group (consisting of the G/S-2, G/S-3, G/S-6, G/S-7, and others). The role of the working group will be to integrate and synchronize cyberspace operations, EW and EMSMO to maintain freedom of action in cyberspace while de-

nying our adversaries the same, ultimately to achieve the commander's operational objectives. This will involve unifying the offensive and defensive aspects of cyber-electromagnetic activities and orienting them on the commander's intent. To this end, the working group serves as the source of cyber-electromagnetic situational awareness and continually assesses progress toward desired conditions.

The first demonstration of the CEMA concept will occur during the Network Integration Evaluation (NIE) 13.1 (Oct-Nov 12) at Fort Bliss, Texas. Representatives from the SigCoE, Army Cyber Command, and MCCoE have already worked with the organizations supporting the evaluation (Brigade Modernization Command, 1st Armor Division, and 2/1BCT) to determine the appropriate network defense related functions that will be conducted in the work group by representatives from the S-6:

- Share and integrate the friendly network common operating picture with information on adversary and other specified cyberspace areas in order to produce overall cyberspace situational awareness
- Receive and request intelligence information from the S-2 in reference to potential threats and associated threat tactics, techniques, and procedures utilized against mission command networks and systems
- Assess, coordinate, and synchronize changes to the unit's information operation condition and

overall readiness level

- Plan, integrate, and synchronize network defense operations into the unit's operations processes and scheme of maneuver
- Report information on unauthorized network activity to be integrated with other possible indications and warnings
- Present a timely and accurate estimate of technical impact resulting from the threat activity and determine detrimental effects to the unit's mission assurance
- Plan, coordinate, and synchronize response actions to threat activity and assess risk for mission command networks and systems
- Plan, request, and coordinate the implementation of network defense capabilities provided by entities external to the unit
- Participate in the after actions review of an incident to determine the effectiveness and efficiency of incident handling
- Assist in the prioritization of CEM effects and targets
- Deconflict network defense operations with unified land operations, to include vulnerability assessments
- Support CEM TTP development
- Assess defensive CEM requirements
- Provide current assessment of network defense resources available to the unit

At least for the S-6, integrating these actions within the work-group alongside complementary functions from the S-3 and S-2 will elevate the commander's support, gain access to information that can proactively lead to the implementation of network defense

countermeasures, minimize risk by leveraging offensive cyber and intelligence capabilities to address threats for which no organic defensive solution exists, and achieve unity of effort. Undoubtedly, lessons learned captured during NIE will determine if the functions stated are correct in fulfilling these objectives.

In the face of new challenges, the Army is indeed losing the fight to defend the confidentiality, integrity, and availability of the information modified, exchanged, and stored by Army networks and information systems.

Recognizing the LandWarNet as part of the cyberspace domain opens the doors to new paradigms and methods to get at this problem. The Army's strength in the land domain undoubtedly comes from its ability to successfully integrate complementary capabilities as part of a combined arms approach. Defending cyberspace should be no different. The ACOIC and CEMA concept will go a long way in making combined arms in cyberspace a reality.

Only the future will indicate if Army leaders adapted at the right time and pace to avoid another painful lesson.

Russell Fenton presently works as Department of the Army Civilian as the Chief of the Cyber Cell, TRADOC Capabilities Management Office Global Network Enterprise, U.S. Army Signal Center of Excellence at Fort Gordon, Ga. He is a retired Signal and Information Systems Management (FA53) officer with over 24 years of combined service.

ACRONYM QuickScan

ACOIC – Army Cyberspace Operations Integration Center
CEMA – Cyber Electromagnetic Activities
CONUS – Continental United States
DoD – Department of Defense
EMSMO – Electromagnetic Spectrum Management Operations

EW – Electronic Warfare
GIG – Global Information Grid
MCCoE – Mission Command Center of Excellence
NIE – Network Integration Evaluation
OCONUS – Outside Continental United States
TTP – Tactics, Techniques, and Procedures

Five Key Cyberspace Defense Elements

By Jac W. Shipp

Why should you care about safeguarding information on your personal, corporate, department, or agency network?

If the information happens to be your personal health or financial information this is a simple question to answer.

For public and private sector organizations, the concern may be over potential loss of proprietary information giving an advantage to the competition. It may be National Security information the loss of which may have a direct impact on our National interests.

The specter of hackers and other cyber threats has received a great deal of attention over the past year through successful attacks on Lockheed Martin, Northrop Grumman, Boeing, Sony, and others. Threats to the safety and security of our personal and organizational data abound. Given what are likely diminishing resources in our fiscally constrained environment, how should we protect ourselves?

If we cannot build a robust defense in depth around our fortress, how can we allocate our resources to dissect, examine, and mitigate the threat?

One plan certainly does not fit all in the realm of cyber security. However, some themes and issues are common across the cyber domain. What follows is a brief discussion of those commonalities with a few suggestions about how to address them and achieve a higher level of data protection. After all, safeguarding the data on our networks is one of the fundamental goals of cyber security.

The scope of our exploration will include five key elements to an effective information-safeguarding program. These elements include system and network users and administrator training and education, the mitigation of external threats, insider threats, threat responses, and situational awareness and understanding.

The authors acknowledge this does not encompass all of the potential threats to your personal or organizational data. Areas specifically not addressed include threats to the air and space links, e.g. intentional or unintentional disruption from interference or jamming, whether of our own design through ineffective frequency management or from adversaries in the form of electronic warfare; disruption in the space link, or space transport layer from sources like space weather, threat space con-

trol activities, or anti-satellite events – intentional or unintentional. We have also not addressed events that cause disruption in the physical infrastructure including cables, fiber, or the supporting power grid. This is not to suggest these are not possible, nor important, they simply fall outside the scope of this work.

To provide a common framework for our discussion on the safeguarding of data we must have a common definition for the word ‘safeguard’ itself. Throughout this work we will use the term as both a noun and a verb. As a noun, we will use the following definition: “a measure taken to protect someone or something or to prevent something undesirable: there were multiple safeguards to prevent the accidental release of a virus.” For the verb form, we will define ‘to safeguard’ as the act of “protecting from harm or damage with an appropriate measure: low interest rates offer the opportunity to safeguard their financial futures.”

User Education and Training

The first of five key areas is user and administrator training and education, particularly in the area of threat awareness. An uneducated workforce spells disaster for protected information. Ignorance of safeguarding techniques leaves room for external threats to penetrate into and escape from networks with valuable information; internal threats to expose sensitive material without challenge; and employees to unwittingly reveal corporate and other secrets.

Even the greatest workforce doubles as an entity’s greatest weakness when unaware of safeguarding techniques.

Workforce training is both the easiest and most effective means to safeguard information. Management should train every employee – not just security personnel – in safeguarding techniques because any employee can encounter a threat or become a threat themselves. The course must emphasize constant vigilance, teach information safeguarding best practices, identify example threats, train employees to identify such threats, and detail prudent threat responses. It would double as a retraining device for those who inevitably make mistakes.

Such training should occur at least every other year. Yes, everyone hates training courses, but they prove effective nonetheless. Successful courses capitalize on the difference between asking students to pay attention and capturing a student’s attention. Employees will leave an interesting

training course with a better understanding of their role in safeguarding information than they had when they arrived. If it is not interesting, courses waste time and resources.

Mitigate External Threats

The second area is mitigation of the external threat. External threats comprise 70% of all network breaches and 98% of all detected network breaches. They come in all forms including electronic phishing and network attacks to physical supply chain and facility breaches. Taking these attacks seriously enables successful defending. Components of external threat mitigation include addressing system and network vulnerabilities, data tagging and encryption, supply chain risk management, and physical security, all reinforced by an effective program of penetration testing.

In this step you must identify system and network vulnerabilities. Some solutions are obvious—add a firewall and patch existing firewalls—but hackers do not limit themselves to conventional tactics. As the Germans did with the Maginot Line in World War II, hackers circumvent firewalls.

To counter adversarial attacks, inspect inbound and outbound network traffic at the packet level. Then run penetration testing on your networks. Hire a red team to hack your network and expose your weaknesses before an adversary exposes them for you. Continue to patrol your network to prevent your defenses from stagnating and to keep adversaries on their toes.

Data Tagging and Encryption Monitoring outbound network traffic also pairs well with data tagging. Tagging every piece of information enables data tracking as data moves through the network, ensuring that only those with predetermined access privileges have information access. The system would quickly flag, stop, and report unauthorized data requests. Tagging should occur whenever a user reads, moves, edits, etc. a piece of data. Data encryption, while common, must be more uniform. Add encryption for data both at rest and in motion. Information is vulnerable when idle or in use, so do not neglect encryption at rest. Adding security layers makes hacking that much harder when stealing your data.

Supply Chain Vulnerabilities

Hardware attacks can ravage your network just as easily as electronic attacks. The entire lifecycle of network hardware and software is vulnerable while it is not in your hands including product conception, design, building, testing, shipping, installation, maintenance, and retiring. If you do not trust those handling your products, you cannot trust the products. During production—especially non-domestic—bad actors can intentionally design “flaws” into products you intend to use giving them unlimited and unmonitored network access to do anything from interrupting internal communications to exposing your most valuable assets. Adversaries might tamper with your products while installing them, during routine maintenance, or even when retiring a product. When possible, buy domestic, trusted products. Otherwise, monitor all vulnerable points as thoroughly as possible. Also consider entering a joint venture with other bodies to sponsor a trusted third party to inspect products and/or companies for you. Individual entities can rarely tackle such massive security challenges alone, but collectively their funds

(Continued on page 24)



(Continued from page 23)

can sponsor someone to tackle it for them.

For physical security establish the best possible physical security practices for your facility. Continue to update your practices as newer and better practices become available. But unless the workforce is aware of those practices, safeguarding efforts go to waste. Keep employees up to date on practices and policies, and how carrying out or neglecting these practices helps and hurts the organization respectively.

Insider Threat

The third key area is the insider threat. The term “insider threat” includes deliberate and unintentional network breaches. While external threats account for 70% of all data breaches, 48% of data breaches—including some overlap—involve insider threats. They begin with employees accidentally or intentionally exposing something due to loose network practices and policies and end with a bad actor either compromising or selling sensitive or proprietary information.

Effective insider threat miti-

gation techniques strike a careful balance between providing information only to those who need it to complete their jobs (Need-to-Know) and distributing information thoroughly (Need-to-Share) for better productivity and situation mapping. Too much of either can prove disastrous. Information distribution first and foremost keeps the workforce aware.

The more information they have, the better they understand the big picture. Waste decreases as employees gain a better understanding of where the need is, how to fill it with their skills, and how to avoid redundancies as bureaucracy falls to the wayside. Information protection is equally important. Limiting individual access to certain data and information types decreases the likelihood of security breaches and successfully ensures individual, information, and asset safety.

The goal is to protect information enough to keep it safe from insider threats while distributing it thoroughly enough to maximize workforce efficiency and support better decision making. Develop a series of standards to help your organization meet these goals. First, ensure

that those who need to know something know it, and those who do not need to will not. Then fill in the gap between the two. Give access to those who could potentially draw connections between different fields or topics and prevent those who cannot and/or should not make connections from getting access. To alleviate this process, establish rules and automate the process to determine who should receive access to what information. Important decisions should always be made by multiple people, not machines, so use the automated access process carefully.

Another aspect of insider threat mitigation is to address the issue of writable and removable media. Flash drives, CDs, DVDs, portable hard drives, and other portable electronic devices provide effective means for transporting harmful software onto and sensitive or proprietary material off of safeguarded networks. Weak network restrictions allow both intentional and unintentional harm to the network by simply plugging in such a device.

If possible, prohibit use of these devices altogether. More realistically, if you cannot, simply limit use of the devices. Require scans of all applicable devices before every use or at least periodically. Limit what information and how information may flow to and from the devices. Finally, log all packets moving to and from the devices in keeping with the data tagging schematic.

	Most Damaging	Most Likely	Overall Priority
Lack of adequate Training and Education	2	1	1
Failing to mitigate External Threats	1	3	2
Failing to Mitigate Insider Threats	3	4	3
Lack of adequate Threat Response Plans, policies, and reporting processes	4	5	5
Lack of Situational Awareness and Understanding	5	2	4

Respond Quickly

The fourth component is having a mechanism for responding to incidents and threats as soon as they are identified. When a security breach occurs, you do not have the luxury of time to figure out how to resolve the problem. Each moment you wait lets adversaries steal additional data, compromise your network further, or even jeopardize your employees' physical safety. Develop a thorough threat response plan ahead of time to minimize the effects of critical periods.

A successful response plan must enable decision makers to make informed decisions about a threat. Therefore, response plans should include the following: threat detection, reporting, analysis, and response. Establish policies covering both external and internal threat response techniques and update them periodically. This process takes a set of initial conditions, passes an accurate summary of the situation to decision makers, analyses threat information to produce viable solutions, and provides the means to create a desired outcome.

A thorough and effective reporting process feeds decision makers' situational awareness and enables situational understanding, or allows them to take appropriate actions with a complete understanding of the consequences for those actions.

Maintain Situational Awareness

The fifth and final component of safeguarding information is situational awareness and understanding. How do you turn situational awareness into situational understanding?

First, establish a baseline for your network by determining exactly what hardware and software your network contains and how the network components connect internally and externally.

Monitor the established baseline for anomalies. Report any anomalies upward to security officials and decision makers before analyzing the incoming anomaly information to determine appropriate response options. Once you have established potential response options, visually represent the network situation for decision makers. This establishes situational understanding by providing decision makers with both an understanding of the situation itself and threat mitigation options. Then select a response and execute through the proper channels.

Unless your organization rehearses these steps regularly, though, your responses will fall apart. Rehearsing works out rough spots in both policy and

procedure, trains participants to respond, and creates second-nature responding. Without rehearsals, a real threat may arise and both insufficient policies and participants who do not understand their jobs will fail to mitigate the threat. Rehearsals should coincide with penetration testing to maximize the benefits of each test.

Unfortunately, it is unlikely we can afford to address everything we have discussed above at one time. To help prioritize our efforts and resources we can apply a risk management approach. The first step is to look at our organization and ourselves from the perspective of a hacker or insider threat. What would they view as most valuable? What would potentially cause the most damage or disruption to our operations?

We can dissect our risk by what is most likely to occur, and most damaging if it does occur. In our example we have set 1=highest, 5=lowest priority/probability. Consulting the USSS report, or your own aggregated information about data loss events within your agency, department, or organization in the past will help in this process.

With this method of prioritization, we can inform the allocation of effort and resources to address all of the key areas, phased in over time, implementing a near-term, intermediate, and long-range plan of action and develop specific milestones to track our progress toward increased information security.

Any organizational data safeguarding plan should include these five key elements. We have examined five key elements that should be a part of any organizational data-safeguarding plan. Their priorities and how you implement plans, programs, and policies associated with implementing these elements must be tailored to your unique data, users, systems, and networks. Employing a risk management process can inform your prioritization process, and should be followed by the development of a detailed plan of action and milestones to support tracking. As you implement your plan, have a set of quantifiable, measurable indicators of effectiveness to support the continuous updating and improvement of your own data safeguarding plan.

Jac W. Shipp, Scitor Corporation, advises various customers on offensive and defensive cyberspace operations. He has planned, led, and supported cyberspace operations for more than 12 years, and briefed cyber issues to the Vice President of the United States, and Directors of the Central Intelligence Agency, National Security Agency, and the Director of National Intelligence.

Join the Discussion
<https://signallink.army.mil>



Engaging two domain warfare

LTC Christopher R. Quick

The Army is now a two domain force--LandCyber and warfighters must embrace the contested domain known as cyberspace.

Since the Secretary of Defense announced the creation of a cyberspace-focused command in 2009, a high demand has been placed on each of the Armed Services to provide cyber resources to support to the Geographic Combatant Commands.

The creation of Army Cyber Command represents as a milestone for the Army on its path to operate as a two domain force in Land and Cyberspace. This event, however, was just an initial step towards solving the larger issues of operationalizing cyberspace, changing the culture, developing a work force, and institutionalizing the Army as a two domain force.

One of the factors driving the transformation is an ever growing and increasingly sophisticated threat. With the diffusion of destructive technology, potential adversaries now pose a greater catastrophic threat to our safety than ever. Relying on low cost stand-off technologies to mitigate our Nation's military might, and coupled with the anonymity provided by the internet, today's complex threats will continue to challenge U.S. interests if we do not embrace the newest domain of conflict.

No longer can we look at our military purely as Soldiers, computers and machines leveraged separately to impose our national will during a physical battle. Soldiers and military vehicles equipped with radios, Global Positioning Systems), smartphones, or other electronic devices must now be considered in the virtual sense as well as the physical.

The use of embedded processors in military equipment carried, driven or flown compels senior leaders to think in a two dimensional, LandCyber sense vice a single physical land domain. In all aspects of operational planning, military leaders will have to engage in physical and virtual (cyberspace) planning before an operation. This will allow our forces to operate unabated in cyberspace.

The second factor driving transformation is the increased importance of network-enabled components in military hardware, which has resulted in a virtual military that few could have envisioned. Technology has always enhanced our ability to prevent, shape, and, when necessary, fight and win our Nation's wars. But with the creation of the virtual Soldier, unit, and their associated equipment, the paradigm has changed and so should the military. The ability to conduct military operations through cy-

berspace means we must be prepared for sophisticated influence operations that leverage cyberspace as a force multiplier and prevent our adversaries from gaining parity. We must, in turn, be prepared to conduct complex cyberspace operations integrated with military operations by integrating capability into force structure.

The U.S. Army must promote increased capabilities within our cyberspace units by populating them with a new generation of digital natives that understands the impact, both real and virtual, digital devices have in today's operating environment. When integrated with digital immigrants - the seasoned veterans who are experienced operating and defending the military's networks through intelligence, computer network operations, information operations, network operations and information assurance - the new generation of digital natives will represent a new breed of Army warrior comfortable with the contested information domain and conversant in cyberspace capabilities.

The Threat

The military's increased reliance on computers and networked devices provides both an opportunity and vulnerability. With the continual expansion of technology and low cost of entry, the operational environment of the future will allow a myriad of threat actors to develop, seize, and exploit advancements in technology. To keep pace with adversaries who rapidly create new and sophisticated ways to capture and exploit data and information. We must understand the risk that comes with the rapid development of capabilities and be prepared to mitigate or accept the risk posed by them.





Today Army warfighters must address the need to operate both on the land and in cyberspace.

Threats in the operational environment (primarily cyberspace) are no longer limited to traditional nation state actors. Instead, they cover potential adversaries that range from rogue individuals to organized groups (like Anonymous and criminal organizations) to sophisticated nation states. The level of sophistication and capabilities presented by this array of adversaries cover a wide spectrum as well. From script kiddies with a laptop or Smartphone engaging in webpage defacement, to attacks like Titan Rain and Moonlight Maze in which U.S. government computers were targeted by organized hackers with access to immense computing power. Collectively, these potential adversaries converge to create a dynamic environment operating outside traditional geographic boundaries and allegiances.

Cyberspace threats also pose a different type of risk than past threats. The span of control in cyberspace creates continuous friction among networks as a range of actors with various af-

filiations, cultural backgrounds, and strategic goals wrestle to control the global domain of cyberspace. The ability to distribute cyberspace assets (both physical and virtual) increases the threat within cyberspace as physical elements (machines and users) cross into the virtual realm using one of many distrib-

uted access points, leverage operational information, and then create realworld (physical) consequences in the other operational domains. This cross domain ability requires commanders to control not only physical access but also virtual access to the critical information and systems used to achieve operational objectives.

Perhaps the most challenging aspect of the threats posed in cyberspace is the difficulty in attributing actions to the responsible actor with any level of certainty or confidence.

Introducing attacks through microwave, thumb drives, portable media, and satellite communications, individuals or teams carrying out attacks can do so remotely, from the safe confines of a neutral, unaware country, while masking their true location and identity through proxies (both man and machine).

While the ability to forensically assess which actor, organization, or nation was behind an attack has improved, the problem remains that the Internet enables anonym-

ity (through virtual personas) that deters security.

Evidence of the changing threat dynamic and the potential for devastating effects can be seen in three examples. The first is an early form of LandCyber in the conflict between Russia and Georgia in August 2008. Georgia's national communication infrastructure, to include government websites, news outlets, and banks, were the focus of a distributed denial of service attack.

People supporting the Russian cause attacked (virtually) immediately prior to Russian military forces entered Georgia's borders for ground operations (Land).

The second example is the attack on InfraGards (a web security partner organization with the FBI) website in February of this year by the Anonymous hacker group. The group stated that "We broke into their web server, perused their assorted presentation materials, and finally deleted everything and vandalized their website."

The last example, which has garnered the world's attention, is the computer attack on Iran's Natanz uranium enrichment plant. The attack resulted from a worm (called Stuxnet) which used four zero-day exploits to disrupt the rotational frequency of the enrichment plant's centrifuges. According to an International Atomic Energy Agency report, this attack severely damaged Iran's nuclear program.

These three attacks highlight several key aspects of cyberspace operations. One, that offensive cyberspace capabilities can cause physical damage; two, such effects can be used independently or in

(Continued on page 28)

In the 21st Century, modern armed forces simply cannot conduct high-tempo, effective operations without resilient, reliable information and communication networks and assured access to cyberspace.

- DoD 2010 Quadrennial Defense Review Report

concert with traditional military operations; and three, that cyberspace presents an opportunity and vulnerability for our Nation's military.

Why a Change is Required

Without a doubt technology has forced a paradigm shift by altering how we view today's operational environment and that of tomorrow.

The ubiquitous presence of digital technology at the tactical level has created a digital presence for each tactical unit, soldier and vehicle that was not thought of before. Just as we seize, retain and exploit the initiative to gain a position of relative advantage in the land domain, we must also do the same in cyberspace.

The increasing array of technology available to individual Soldiers, from biometrics to global positioning systems to Smart phones and tablet computers, means that wherever the soldier is in the world, cyberspace follows, as do its inherent risks.

The use of embedded processors in military equipment - whether carried, driven, or flown - compels military leaders to think in a two dimensional (LandCyber) sense vice just a physical domain (Land) sense.

In all aspects of operational planning, military leaders must now consider both the physical and virtual (cyberspace) domains when planning an operation. The transition from Soldiers with a tactical radio and map to LandCyber soldiers with multiple electronic and digital devices represents the evolution of two dimensional Soldiers whose virtual persona must be factored along with their physical presence. Commanders must understand their units' digital persona as well as the physical, and that their command can be virtually tracked, located, attacked,

and destroyed just like the physical unit can.

Voice and data networks that once operated separately have converged and now enable the delivery of multiple forms of media - text, audio, and video - over the same wired, wireless, or fiber-optic infrastructures of the Internet. The benefit of this converged Army network is that it functions as a central nervous system for every unit, connecting leaders to their forces. The ability to communicate, see the battlefield, and maintain situational awareness depends on access to the Army's networks. Not only must the commander account for his digital persona, he must also ensure confidence in the integrity of the network while engaged in the contest of wills. Thus, the cyberspace contest is not an ethereal struggle, but an integral element of a units' ability to shoot, move, and communicate.

While technology improves conditions for the ground commander to achieve the stated objectives, connecting to today's networks also connects the commander and the unit to other friendly, neutral, and adversarial audiences and actors.

This means cyberspace enables commanders to better visualize, describe, direct, lead, and assess the operational environment by giving them greater access to reliable information. In short, LandCyber enables mission command by helping commanders and their staffs better assess the character and impact of the information environment in their operational area. To fully benefit from this improved information awareness, commanders and their staffs must understand cyberspace as a 'combat arm.'

Lastly, the Army has been directed, (in the Department of Defense Strategy for Operating in Cyberspace) to focus on three areas of potential adversarial activity: theft or exploitation of data; disruption or denial of access or service that affects the availability of networks,

information, or network-enabled resources; and destructive action including corruption, manipulation, or direct activity that threatens to destroy or degrade networks or connected systems. Leaders, however, lack sufficient situational awareness and understanding of cyberspace to manage risks and exploit opportunities. The Army has no common level of Soldier "digital awareness" across its ranks.

Keeping Pace with Technology Changes

The operational environment contains a wide range of clever, adaptive adversaries who can impact the Army's networks with small-scale technologies. They collect intelligence on the U.S. to determine vulnerable IP components and electronic apertures for key systems and highly selective cyberspace, electronic, and kinetic takeouts of key nodes. They can influence our national will and decision cycle through social media, internet chat rooms, blogs, and international media. Their ability to impact a military operation through cyberspace means we must be prepared for sophisticated influence operations (both kinetic and non-kinetic) that leverage cyberspace as a force multiplier and prevent our adversaries from gaining parity. To be prepared to conduct complex cyberspace operations integrated with military operations, we must integrate capability into force structure.

Technology has always been considered an enhancement to our ability to prevent, shape, and win the wars of the U.S. But as the creation of the virtual soldier/unit and associated equipment has changed, the paradigm, the military must also change. Operations in cyberspace can occur nearly instantaneously. Army forces can attack or be attacked in cyberspace at a rate not achievable in the other domains. Depending on the degree

of interconnectivity, this can happen over vast distances at near the speed of light. The tempo in which these activities take place poses a requirement for speed in decision making heretofore not known or required. Legacy processes, methods, and equipment must yield to new concepts and equipment that compensate for the fluid, dynamic, and contested domain of cyberspace (must be based on people, technology, and applications).

The United States has created, developed, and deployed many innovations in the hardware and software sectors during the information age. Yet other countries now move just as quick in technology sectors and their ability matches or exceeds ours in some arenas. To maintain our advantage in the information environment, the US military must synchronize tools, personnel, protocols, and machines into rationally persuasive systems that can effectively operate at network speed.

An efficient use of a system of systems (man, machine, and applications) will promote finding, fixing, mitigating and resolving threats to our networks and military operations.

Successful operations will require the development of integrated cyberspace intelligence collection capability with cyberspace operations to facilitate mission command and operational effects across the other warfighting domains. With multiple opportunities to inflict damage through malicious activity, the actions of a few individuals has forced a paradigm shift in how commanders view mission command as well as preserve the rapid free flow of information sharing required in today's environment.

ADP 3-0 (dated October 2011) states that "Unified land operations describes how the Army seizes, retains, and exploits the initiative to gain and maintain a position of relative advantage in sustained land operations through

simultaneous offensive, defensive, and stability operations in order to prevent or deter conflict, prevail in war, and create the conditions for favorable conflict resolution." The Army, however, lacks sufficient cyberspace capability and capacity, as well as the integrated Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities construct necessary to effectively support commanders accomplishing this task as part of the Army's Prevent/Shape/Win strategy. Developing an integrated LandCyber construct will better inform commanders and staffs how to support not only the Army but Joint requirements as well.

We must devise a "Smart Defense" approach to pool, share, and specialize capabilities as needed to meet 21st century challenges. Leveraging the Next Generation While technology plays an important role in the cyberspace, it is not the technology that will win on the 21st century's cyberspace battlefields. Rather, people will make the difference. The U.S. Military must cultivate cyberspace units by populating them with a new generation of digital natives who understand how digital devices influence both the real and virtual environment. These digital natives will use their knowledge of the dynamic rules and culture of cyberspace to enhance the ability of leaders/commanders to achieve their military objectives. The U.S. Army must recruit, develop, and retain skilled, professional Soldiers (active duty and reserve component), and DA civilians in a highly competitive environment.

The development of LandCyber Warriors to gain physical, temporal, and psychological advantages over an enemy will enable us to execute cyberspace operations from people-built cyberspace war fighting platforms. Teams of cyberspace warriors will use these cyberspace platforms to support both Army and Joint requirements.

We do not yet, however, have the human capital or authorities to make all this work.

As the demand for cyberspace personnel has increased so has the challenge of retaining personnel with current skill sets.

The Army must create (or modify existing) talent management processes to leverage current Soldiers and civilians with pronounced learning aptitude and problem solving skills. This will allow the Army to focus existing personnel with cyberspace-related attributes on tasks derived from DOD Global Information Grid Operations, Defensive Cyber Operations and Offensive Cyber Operations. However, the overall cost of this endeavor is a greater monetary cost to develop a skilled cadre. As discussed at the March 2012 Land Cyber Summit: Additional skills + additional training + more senior positions = higher dollar cost per individual.

Although our Nation faces serious challenges in access, training, developing, and retaining Soldiers and Civilians to effectively operate in cyberspace, the current work force provides an interim solution. This solution involves the utilization of current Army professionals in the Intel, Signal, EW and IO communities who have desired cyberspace skill sets and expertise. These skill sets include 35Qs, 35Ns, 35Ps, 352Ns, 352Ss, 353Ts, 255Z, 255A, 255N, 255Ss, 25As, FA26s, FA29s, 290As, 29Es, FA30s.

These personnel can provide the initial framework for establishing cyberspace/electro-magnetic Cells at ASCC down to brigade level and for building cyberspace warfighting formations and headquarters.

To address its shortage of trained cyberspace personnel the Army should use the wide range of existing opportunities in the personnel inventory today.

(Continued on page 30)

(Continued from page 29)

These opportunities (bonuses, reclassification, assignment of choice) will require adequate resources and modification (must measure aptitude and potential technical skill) to be properly used in support of enhancing effectiveness. Additionally, by packaging on-going efforts into a comprehensive cyberspace recruiting strategy, the Army can adequately address and remedy its recruit, train, and retain gaps.

Paramount to any cyberspace workforce solution is the inclusion of tailored civilian management process. Current information and tracking systems are insufficient to support detailed understanding, identification, assignment, management and tracking.

There are positive attributes associated with the Civilian workforce excepted and competitive services; however, neither program is sufficient by itself, which requires further analysis.

Last, the cyberspace workforce should have access to training from a variety of venues that offer a common educational platform/portal that provides robust environments to develop and enhance skills of the force. Access to training should include virtual ranges and training environments that simulate challenges that test individuals and team capabilities. This capability should encompass the ability to access operational SME's and leaders that can facilitate train-

ing in either institutional or operational environments.

Conclusion

Without doubt the Army is now a two domain force (Land-Cyber). As such, it must embrace cyberspace as an operational domain. Army Cyber Command provides the foundation from which the Army can leverage its ability to operate in Land and Cyberspace. However, since we have transitioned to LandCyber, the Army can no longer look at its forces purely as Soldiers, computers and machines that are leveraged separately to impose our will during battle.

The long list of potential adversaries with the capability to pose catastrophic effects will continue to threaten U.S interests if we do not face and embrace the newest domain of conflict. The growing number of Soldiers and military vehicles equipped with radios, GPS devices, and other electronic devices demand consideration in the virtual sense as well as the physical.

The two dimensional ideology (LandCyber) must permeate the decision cycle and operational planning of military leaders if we are to prevent, shape, and when necessary, fight and win our Nation's wars. The ability of our adversaries to impact a military operation through cyberspace demands that the Army prepare for sophisticated influence operations that leverage cyberspace and

prepare to conduct complex Land-Cyber military operations.

Finally, the U.S. Military must cultivate cyberspace units by populating them with a new breed of digital natives comfortable with digital devices in the future information environment both real and virtual. Combined with seasoned digital and information veterans who have operated and defended the militaries networks the Army will not only successfully operate in cyberspace, but become Second to None in Cyberspace.

LTC Christopher R. Quick is currently the Director of Strategic Communications for the U.S. Army Cyber Command / Second Army at Fort Belvoir, VA. His assignments include Fire Support Officer, Battery Executive Officer, Brigade Assistant Operations Officer, and Brigade Fire Direction Officer. He commanded a Battery with 1st Battalion, 17th Field Artillery. He served in the 41st Signal Battalion, 1st Signal Brigade as a Battalion Automations Officer. LTC Quick served as Brigade Information Operations Officer with the 2nd Brigade, 101st Airborne, where he served a tour in Iraq. He has served on the Army Staff within the Army G3/5/7 in DAMO-ODI and served on the Army Cyber Task Forces as the lead action officer for the development of Army Cyber Command. LTC Quick holds a B.S. degree from Park University in Kansas City, Mo. and an M.S in Computer Science and another in Information Operations from the Naval Post Graduate School in Monterey, Calif.

Join the Discussion
<https://signallink.army.mil>



ACRONYM QuickScan

C/EM - Cyberspace/Electro-magnetic
DCO - Defensive Cyber Operations
DDoS - Denial of service attack
DGO - DOD Global Information Grid Operations
DOTMLPF - Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities

FBI - Federal Bureau of Investigation
GCCs - Geographic Combatant Commands
GPS - Global Positioning Systems
OCO - Offensive Cyber Operations
SME - Subject matter Expert

Rigorous cyberspace defense expert training moves forward

By CW4 Ivery Torbert

As I write this, there are 12 Soldiers sitting in modular building 8C on Fort Gordon learning and practicing skills that will prepare them to be experts in gaining freedom of action in cyberspace.

Like the four that preceded it, the current class includes a mix of CW2's and CW3's. This is the fifth iteration of the course comprising active duty, National Guard, and Army Reserve Warrant Officers. Unlike classes of the past, this one has two senior non commissioned officers hopeful of becoming the first 25D enlisted cyberspace defender.

Military occupational specialty 255S, cybersecurity technician, is arguably the most challenging cyber professional military education and MOS qualification at the U.S. Army Signal Center of Excellence, if not across the Army and Department of Defense. To that end the SIGCoE created an accession process for those seeking to challenge this curriculum. A candidate must be a graduate of a Signal warrant officer basic course, be at least a senior CW2, possess a DOD 8570.1-M information assurance technical Level III certification, have documented cyberspace operations work experience, possess a current top secret-SCI security clearance, and be prepared for the most challenging course of their careers.

Warrant officers selected for training will gain access to an on-line security essentials course for 14 days and be required to take the GIAC security essentials certification on day 15. The GSEC certification is not a prerequisite, but serves as an entrance exam. Statistics indicate that candidates that do well on the GSEC have done well over the 25 weeks that make up the 255S curriculum. Failure of the GSEC certification does not disqualify candidates from seeking the 255S program, but it will place you at a disadvantage compared to candidates that meet all the prerequisites and pass the GSEC.

The intent of course managers is to graduate a capable, fully trained officer from the 255S program. We are currently partnered with the SANS Institute and they provide approximately eight weeks of our resident training. The SANS instructors and course material are second-to-none. The classes are filled with the type of hands-on learning and validation that support the future Army Learning Concept. In addition to the resident course, students are given access to SANS on-demand portal with online access to

the same material covered during that training week.

Students can also download audio files of the same lecture to mp3 players or DVD. Students have to complete exercises associated with all the SANS training created by 255S resident instructor. Most of the training is hands-on and meant to enforce and/or demonstrate learning from the previous week. The course has three Capstone events: Phase I, Phase II, and Capstone exercises. Students also compete in a minimum of three capture-the-flag type events that demonstrate their ability to gain access to and maintain access on a target system. In one CTF, PY-WARS, students get to write and execute their own code.

The 255S course is professional military education. Graduates of the course are awarded Warrant Officer Advanced Course credit. It also serves as MOS qualification course when specific gates are met. It is possible for a Soldier to come to Fort Gordon to challenge the course and leave with WOAC credit only.

Beginning in January 2013, Soldiers will have to test and pass TRADOC exams before being allowed to take an industry certification. If the Soldier fails the TRADOC exam, they risk expulsion from the 255S WOAC and would possibly be slotted in the next available 255A/255N WOAC.

Soldiers that pass TRADOC exams will move on to challenge industry certifications. Soldiers will take the Global Information Assurance Certification, Certified Windows Administrator, GIAC Certified Intrusion Analyst, GIAC Certified Incident Handler, GIAC Certified Systems Auditor, GIAC Certified Forensic Analyst, and GIAC Certified Penetration Tester.

The tools and capabilities given to these Soldiers are difficult to learn, let alone master, so this makes the accession process extremely vital to the future success of the student. Candidates have to be scrutinized to protect the Soldier. This course requires tremendous dedication and focus.

Candidates should not take the course lightly. Under the current Course Management Plan, students have to pass four of six GIAC certifications offered and complete all WOAC requirements to graduate as a true 255S. Of the four GIAC certifications, GCIA and GCIH are mandatory. The skills

(Continued on page 32)

(Continued from page 31)

trained during these two courses and during the Basic Computer Network Operations Planners' Course make up the core foundation of what we believe 255S will do for commanders in the field. Failure of certifications will not get you removed from the course as long as the effort remains consistent.

A core component of the 255S course is the Basic Computer Network Operations Planners' Course. This course prepares planners to integrate computer network operations into the commander's operations down to the tactical edge. Aspects of CND by themselves are functions of all Signal skill-sets.

Protection is a key component of the Signal Warrant Officers' duty. Network technicians should never engineer networks without taking into account firewall placement and management, intrusion prevention systems, content filtering, IDS, encryption, remote access, and basic computer network defense.

Systems technicians cannot place automation systems onto that network without accounting for patches, anti-virus, firewall, backups, host IDS, host IPS, ports and protocols, encryption, remote access, or basic security and network defense. By taking from this force that is immersed with defensive talent, we can focus the training for 255S on more offensive tactics that can be used to better understand the threat and proactively find and fix vulnerabilities before any threats can exploit them.

One option offered to candidates who excel, is to take Global Information Assurance Certified Security Expert exam prior to graduation from the course. The GSE exam has two parts. The first is a multiple choice exam which may be taken at a proctored location just like any other GIAC exam. The current version of the GSE multiple choice exam has



Photo by Cotton Puryear, Virginia National Guard Public Affairs

Cyberspace network defense is a top priority throughout the Army. Here Soldiers from the Virginia National Guard Fairfax-based Data Processing Unit conduct a computer network defense exercise 15 Sept. in Fairfax. The exercise used different cyber-scenarios of varying difficulty in order to evaluate the proficiency levels of the unit's Soldiers in computer network defense and was also designed for senior leaders to evaluate the effectiveness of cyber-warfare training provided during the 2012 fiscal year. The 255S MOS Course is the U.S. Army Signal Center of Excellence training designed to provide the cyberspace defense experts the Army needs.

the passing score set at 75% and a time limit of 3 hours. Passing this exam qualifies a person to sit for the GSE hands-on lab. The first day of the two day GSE lab consists of an incident response scenario that requires the candidate to analyze data and report their results in a written report. The second consists of a rigorous battery of hands-on exercises.

To date the SIGCoE has paid for nine candidates to take the GSE written exam and all passed. Students do not have enough time to attempt the lab prior to graduation. Upon certification as a GSE,

Soldiers only have to recertify as GSE to update all previous GIAC certifications. All students who successfully complete the GSEC and the two core courses are eligible to challenge the GIAC GSE.

The 255S MOS is an accession MOS. It is comprised of former 251As, 254As, and 250Ns. Yes 250N.

A prevailing thought in the force is that we are graduating Warrant Officers who will go out and fill information assurance roles. However, that IS NOT the purpose of the training Soldiers are getting here.

Having a “cybersecurity” expert in the force DOES NOT eliminate the inherent IA responsibilities of network/system administrators and users. We are pulling Soldiers with IA skills because they understand what is happening in computer network defense.

We want Soldiers who understand and comply with the standards technical implementation guidelines. We need Soldiers that are responsible for firewall management and access list creation on multiple tiers.

If you currently are an ePO administrator; write IDS/IPS signatures; work with RADIUS, VPN, IPSEC; perform scripting; or like playing with Linux in your spare time, then we are looking for you.

Remember this is an advance course with the focus on cyberspace operations and not IA compliance.

The 255S course has had four total graduating classes to date. The first class was considered a train-the-trainer which was followed by three pilot courses to validate our program of instruction. We have trained 38 active duty, 10 Army Reserves, and seven National Guard Signal warrant officers.

Much is made of the certification obtained in the course. Our primary focus is to graduate trained cybersecurity technicians capable of supporting operations throughout the cyberspace domain; however, until we have a cyber workforce, which by designation of MOS has the full respect and trust of Army leaders, one needs to have credentials.

The certifications serve to validate skills. Without knowing exactly at what echelon 255S will be placed in the force, we chose multiple disciplines for specialization. They are trained in areas such as: hacker techniques, incident handling, auditing of networks systems and perimeters, advanced computer forensics, intrusion analysis, network

penetration and exploitation, Linux/Unix security, virtualization security, Windows security; cyber law and ethics, and even python scripting.

In January 2013, we are adding malware analysis and mobile forensics to the course. As mentioned earlier, students will take six total GIAC certifications during their stay at Fort Gordon; and they must pass four of six to graduate as a qualified 255S.

Who pays for recertification? With Soldiers obtaining so many certifications it will be a challenge to maintain them all. The hope is the Army will support future certification funding in order to maintain a highly skilled, operational cyber workforce. Until then, Soldiers may have to engage their units to stay current in their credentialing related to the mission of the unit. Ultimately, senior Army leaders will address this issue. Currently, educators at the SIGCoE are primarily charged with meeting individual training requirements that create Soldiers who can prevent, shape, and win in cyberspace.

The nature of threat and the Army’s dependence on cyberspace to enhance operations has caused a change in the type of Soldier and training the Signal Regiment provides. With this second-to-none training, we are creating Soldiers who specialize in looking beyond the green, red, and amber status of the network. Graduates of this course will leave with a better appreciation of cyberspace by looking at it in a different fashion; and understanding what it will take in the future to prevent, shape, and win in a dynamic operational environment. As the Signal Regiment expands its role in cyberspace operations in order to meet the needs of the nation, 255S are leading the way. This rigorous course is well worth the effort.

CW4 Ivery Torbert currently serves as the Computer Network Defense Branch Chief, 442nd Signal Battalion, Fort Gordon, Georgia, which is responsible for the 255S Information Protection Technician course, he is also a graduate of the first 255S class October 2010.

ACRONYM QuickScan

CND - Computer network defense

CNO - Computer network operations

CTF - Capture-the-flag

DoD - Department of Defense

GCWN - Certified Windows Administrator

GCIA - Certified Intrusion Analyst

GCIH - Certified Incident Handler

GSNA - Certified Systems

Auditor

GCFA - Certified Forensic

Analyst

GPEN - Certified Penetration

Tester

CMP - Course Management Plan

GIAC - Global Information

Assurance Certification

GSEC - Security Essentials

Certification

GSE - Global Information

Assurance Certified Security

Expert

IA - Information assurance

IPS - Intrusion prevention systems

MOS - Military Occupational Specialty

POI - Program of instruction

STIGS - Standards technical implementation guidelines

T3 - Train-the-trainer

TRADOC - U.S. Army Training and Doctrine Command

SIGCoE - U.S. Army Signal Center of Excellence

WOAC - Warrant Officer

Citizen Soldiers ready to defend cyberspace

By MAJ Aaron Munn and John Galeotos

Human capital and ingenuity have been and still are one of our nation's most precious assets. We are a nation of leaders, scientists, technological innovators, and corporate visionaries with diverse backgrounds and beliefs; and nowhere in the military is this diversity so embraced as it is in the ranks of the National Guard. A Citizen Soldier not only brings to the fight the same high levels of integrity, loyalty, professionalism, and duty as their active duty counterparts but, they also cultivate a diverse spectrum of civilian skills and experience that he or she provides during drills or deployments.

In today's modern society, the additional skills that the citizen Soldier brings to the table along with their military occupational specialty training are becoming increasingly technical in nature. It is not at all uncommon to find a Guardsman, who as a civilian, works for an intelligence agency or information technology contractor, a computer manufacturing or software programming corporation, or work in another related high tech field.

The Guard appeals to this patriot; they are leaders in their professional life with successful jobs or businesses, but they also want to serve our nation to feel a sense of pride in performing their duty and the esprit de corps that comes from serving with other noble men and women.

Those in the National Guard are prepared and trained to defend our nation for domestic and overseas contingencies. These ready and adaptable forces present additional capacity and capability that must be leveraged for defending Department of Defense, as well as federal and state government networks. In many cases the Guard is already part of the cyber fight through "Access," "Capability," and "Experience" to operate in this evolving environment.

Access

The National Guard is in each state and territory as well as The District of Columbia. It is this access at the local levels that enables the National Guard to execute cyber missions where other agencies have difficulty. This distribution of forces has obvious advantages for domestic response options and by defending networks at a local level the nation's cybersecurity

posture is bolstered. Additionally, the citizen-Soldier works in the cities and towns where private industry, corporations, and local, state organizations will also benefit from their training and expertise.

National Guard leaders have developed strong relationships with state emergency response entities that provide assistance in the event of crisis situations in the physical world; and it is those relationships that are being leveraged to increase the Guard's capability to assist local first responders in

the event of a crisis within the notional world we call cyberspace.

These relationships as a matter of public safety and national security must be shaped and formed to develop cyber incident response plans and contingencies because, as abstract an idea cyberspace is, it touches nearly every part of our daily lives.

Currently, these relationships between the National Guard and their state and Local governments are being drafted, refined, and socialized to expand the individual efforts into a national capability. These efforts identify policies, authorities, roles, and responsibilities for National Guard cyber-capable forces to prevent or recover from possible catastrophic effects of a cyber-attack. As state National Guard units establish integrated cyber incident response plans with their local authorities, our cybersecurity as a nation grows.

The National Guard also has its' federal relation-



ships with Department of Defense. The National Guard's relationships with both state and federal organizations provide unique opportunities to facilitate cyber incident response options that can be leveraged for local and national requirements. Ultimately, the National Guard's access within state, federal, and Department of Defense organizations can provide an integrating function for our nation's cybersecurity efforts and provide value to the advancement of a cyber-common operating picture shared between state and federal entities.

Capability

The Guard currently has cyber forces conducting both defensive and offensive cyber operations in Title 10 USC and Title 32 USC status. These forces are generated from a mix of Signal, Military Intelligence, Information Operations, Electronic Warfare units, as well as Air National Guard Cyber units. The elements range in size from squad to company size, so capabilities can vary dramatically per command.

In addition to these domestic and federal capabilities, the National Guard has international partnerships. The State Partnership Program matches individual state National Guards with sister nations to promote long term, enduring and mutually beneficial security relationships with friendly and allied nations around the globe.

The National Guard SPP provides forces to the Combatant Commands that encourage international cooperation and understanding, develop enduring relationships, and build mutual capacity to tackle the world's toughest challenges – to include cyber. The U. S. European Command has the most mature cyber SPP with eight of its twenty-two SPPs actively involved in cyber engagements with their sister nations. The National Guard states involved are Alabama, California, Colorado, Connecticut, Indiana, Maryland, Michigan, Minnesota, North Carolina, Nebraska, New Jersey, Ohio, Pennsylvania, New Jersey, Tennessee, Virginia and Vermont have all conducted exchanges with their partner nations.

Recently, the Virginia Army National Guard's Data Processing Unit, a cyber-capable unit located in Fairfax, Virginia, and the United Kingdom's Land Information Assurance Group, demonstrated a model for an effective first-of-its-kind cyber exchange. This exchange enabled each participant to learn how the other addressed cyber defense and to train together in an environment where the gaps could be identified and bridges built; both technical and policy in nature.

The exchange was conducted in two phases. In the first phase, the United Kingdom and National Guard Soldiers attended training on Camp Robinson, Arkansas at the Army National Guard's Professional Education Center, and then ended their engagement in Virginia.

This training consisted of familiarization with the Army National Guard's cyber simulation environment, providing operator level familiarization as well as high level system architecture exposure to understand how the flexibility of simulation platform could be adapted to various training requirements. In Virginia, the two units conducted a cyber exercise where they focused on detecting threat traffic and implement mitigation techniques.

The exercise scenarios ranged from denial of service attacks to various different means of data exfiltration to attacks against email and other critical system services. Multiple scenarios were run against the team often simultaneously. The next part of this exchange will take place in the United Kingdom. The Virginia DPU will travel to the United Kingdom sometime in early Fall 2012 and conduct a reciprocal event.

Even though many of the questions that complicate the military's role in the defense of cyberspace are still to be answered, the Guard continues to make progress and grow capability in spite of the numerous difficulties presented by outdated public policy and laws that create legal gray areas. The Guard's unique command structure enables its forces to individually address how they will respond to new cyberspace operations missions. The flexibility is evident in the diverse organizational structures that currently exist within the Guard in response to this problem set.

Experience

Some of America's most significant scientific advances, innovations, trade secrets, formulas and algorithms exist simply as data stored and processed on our nation's networks. How do we protect these incredibly valuable intellectual assets; especially with the difficult and complex landscape we call cyber? As it has been since the birth of our nation, the National Guard stands ready to answer this call.

It is important to understand the focus of the National Guard's efforts when we discuss cyber missions. The National Guard supports both domestic and federal missions. This dual-use function is the essence of what defines the "Guard" and distinguishes its ability and access to support cyber defense and response to defend the homeland. When a hurricane or wildfire threatens the citizens of a state, the experience is something very tangible, frightening, and occasionally tragic. In these situations, the citizens of our great nation welcome the assistance and protection of the National Guard, in fact they assume the Guard will be there and ready to respond. For over 327 years, the "Minutemen" have been there.

The cyber threat is subtle and insidious. It's not an enemy trail you can easily observe with your eyes.

(Continued on page 36)



"We will work with all the key players - including state and local governments and the private sector - to ensure an organized and unified response to future cyber incidents. Given the enormous damage that can be caused by even a single cyber attack, ad hoc responses will not do. Nor is it sufficient to simply strengthen our defenses after incidents or attacks occur."

- President Barack Obama - May 29, 2009

(Continued from page 35)

It is not a rolling grey plume of dust devouring our cities. It is a difficult problem set that requires a different approach from responses to physical events like earthquakes or fires. The recovery from a large scale cyber attack is not as straight forward as a truck loaded with supplies after a hurricane or a plane filled with fire retardant to engage a wildfire. None-the-less the response to a major cyber attack is a mission that we must support because it is vital to the security of our nation.

In President Obama's speech on cybersecurity, May 29, 2009, he states "We will work with all the key players -- including state and local governments and the private sector -- to ensure an organized and unified response to future cyber incidents. Given the enormous damage that can be caused by even a single cyber attack, ad hoc responses will not do. Nor is it sufficient to simply strengthen our defenses after incidents or attacks occur."

The Guard has the experience needed to accomplish this mission. The Guard is already there.

Summary

There are many challenges ahead of us as we address the com-

plexities of operations in cyberspace. Beyond what types of cyber units are needed to fight the fight, recruiting, training, and retaining the highly skilled workforce needed in order to conduct cyberspace operations is daunting. Cyber can be considered a specialized craft and in order to grow cyber capability and capacity, it will require innovation in many ways to include retention. Arguably, the cyber profession may need to be treated like Aviators and pilots, doctors, or Special Forces operators: highly specialized and in high demand. These professions have tailored programs providing mechanisms to improve overall retention; cyber may and perhaps should have the same approach and philosophy.

The Guard is where these forces are needed. For over three centuries the Guard has favored its civilian nature in peace and donned the fierce aspect required during times of war.

John Galeotos, CISSP, CCNA Se-

curity, works for CACI International Inc. as a cyber subject matter expert. He is also a CW2 251A in the District of Columbia National Guard as a CND-team chief. He has worked for the Wyoming Army National Guard, White House Communication Agency, Department of Commerce, and currently at the National Guard Bureau in Information Management Governance on the ARNG Cyber Working Group.

MAJ Aaron Munn is currently serving as Army National Guard's cyber operations project officer. His military background and qualifications include information operations, public affairs, Signal, and air defense. MAJ Munn has served in the Army National Guard for over 20 years with assignments in three states and three mobilizations. His civilian experience includes high tech investigations, information security, and network administrator. He is a Certified Information Systems Security Professional, Microsoft Certified Systems Engineer, and A+ Certified Technician.

ACRONYM QuickScan

DPU - Data Processing Unit

USC - United States Code

SPP - State Partnership Program

Redefining Information Assurance compliance

By LTC Christopher Quick

Cyberspace has and will continue changing the way we all conduct our Profession of Arms. This applies to everyone--the Infantryman, the Signaler, the intelligence analyst and the commander in the field.

Global connectivity and the speed at which information is transmitted around the earth have fundamentally altered our world, and we cannot go back to how things were.

Technology continues evolving to meet today's threats while simultaneously building toward the future. Our task is to understand the dynamics driving this rapid change and stay ahead of the malefactors loitering in the shadows and acting to impede our progress.

The keys to information assurance are understanding and mitigating risks.

We can accomplish this by implementing standards, correcting deficiencies, and enforcing modes of user behavior, currently known as compliance. The discipline and standards bedrock undergirding our Army must be carried forward into the cyberspace domain.

Compliance in Information Assurance is one of Army Cyber Command's most pressing and important mission imperatives. It is a multi-dimensional term subject to wide interpretation in its application.

Driving this vital imperative are cyberspace threats that are real, growing, sophisticated, and evolving. As we work to take full advantage of cyberspace's potential, we must recognize existing and future threats and appreciate their ability to prevent us from operating freely. Threats include a wide set of actors with digital devices or computers



Global connectivity and the speed at which information is transmitted around the earth have fundamentally altered our world, and we cannot go back to how things were.

trying to improperly access our enterprise with nefarious intent.

Trend analysis indicates the number and sophistication of attempts to exploit our networks will continue to increase and mature. We must anticipate the evolution of these threats. Every time we enter the network, regardless of where we are, we are in a contested environment in which we must fight to maintain our freedom to operate.

Since its creation, Army Cyber Command has actively focused on operationalizing Computer Network Operations. IA compliance is a key part of this process.

However, there are unique challenges in doing so, including the volume of IA threats and vulnerabilities, the escalating pace and sophistication of emerging threats, the distributed and dispersed state of current Army networks, a general lack of security training and awareness, and a traditional lack of leader-

ship understanding and involvement in actively implementing required IA implementations.

In addition, the command has worked to reduce the frequency and systemic causes of costly IA compliance failures, such as unauthorized disclosures of classified information (UDCI, formerly known as "spillage"). In all, operational emphasis on Information Assurance compliance has led to tangible improvements in security and user awareness. Much, however, is still required of Army Cyber Command, the cyberspace community of interest, and Army leadership to mitigate risk and deny adversaries access to the Army's sensitive information.

Why Information Assurance Compliance?

The better question to ask is why compliance with Army orders and directives? The primary reason for enforcing

(Continued on page 38)



(Continued from page 37)

Army-wide standards and user norms is the need for a strong defense. Protecting information and guaranteeing transportation through cyberspace is essential to how our Army fights.

The ability to operate when degraded or disrupted provides significant advantages to the side that can gain, protect, and exploit advantages in the contested cyberspace domain. The advantage will go to whoever best mitigates the loss of intellectual capital and reduces the number of vulnerabilities.

In some cases improved defense results directly from short term actions taken to diminish known threats, such as the application of a vendor patch. In other cases, improved defense results from the gradual implementation of enterprise-wide applications that move the LandWarNet (the Army's network) toward a more uniform and interoperable network.

For example, migrating to a common Windows platform or synchronizing the tuning of Host Based Security System may not give the immediate appearance of defense; but these important actions promote a more automated and thus more responsive network. Without these common configurations, the network cannot effectively feed the emerging common operational pictures, such as IT asset management or continuous monitoring.

We can neither afford the loss of critical information, nor afford the cost of remediation. A clear example of this is in the area of UDCI, where an entirely avoidable act can result in a sizeable remediation price tag for the unit involved. This year remediation costs exceeded \$700,000. That is unacceptable.

Most important, however, is that comply-

ing with orders and directives is not voluntary. As with any Army operation or task, orders and directives must be followed. Just as with any mission or operation, failure to accomplish assigned tasks can jeopardize the overall mission. This is critically important in cyberspace operations because cyber enables mission command.

What is Army Cyber Command doing?

Army Cyber Command is actively moving forward with operationalizing IA compliance by regimenting the orders process and helping commanders mitigate risk by prioritizing vulnerability remediation to address the most critical enterprise vulnerabilities first. This process allows field commanders to see risks in operational terms so they can understand impacts to their units and take action based on operational needs.

Consider the case of the UDCIs described above. Since reaching a monthly high in February 2011, poor user behavior has declined 50% to the end of October 2011. Command emphasis and outreach reduced the frequency and severity of these events; more work, however, is required. Commanders at all levels have come together with a common sense of urgency to correct the problem.

Where orders implementation is concerned, one process in particular is putting a fine point on compliance. Dubbed the "High Risk Vulnerability List," this new breed of order identifies the most widespread and potentially debilitating vulnerabilities in the Army and mandates they be addressed immediately. Their status is reviewed weekly, with focus on a manageable set of vulnerabilities versus the full continuum of active vendor patches. Anecdotal responses from the field have been positive, as this "High Risk" order estab-



A new breed of order identifies the most widespread and potentially debilitating vulnerabilities in the Army and mandates they be addressed immediately.

lishes a common priority of effort based on command direction.

Cyberspace operations orders also work well in high profile cases where the Army must act immediately and decisively in the face of emerging threats. On the heels of the Wikileaks incident in late 2010, for example, Army Cyber Command issued the single codifying order that aligned all mitigation actions; units subsequently reported full compliance within weeks of the release of the order. This single recognized orders process continues to pay dividends across a broad range of deliberate actions, from Enterprise E-mail to the patching and scanning of Army systems.

Army Cyber Command has also established a recurring command forum for the assessment of other compliance indicators. The monthly Cyberspace Operations Readiness Report brings all components together to discuss the status of orders implementation, cyber security training, "High Risk" vulnerability implementation, and the results of external inspection.

It is this last compliance element where Army Cyber Command stands poised to make a fundamental difference. For too long the Army's information security inspections have been "fire and forget" events that might have received attention early on, but then faded into obscurity soon afterward. Army Cyber Command has taken the lead role in de-conflicting the numerous IA inspections pending at any given time by various organizations (e.g., Defense Information Systems Agency, Command Cyber Readiness Inspections, Inspector General, and Army G3), and is aligning the full Army audience to a concise list of candidate sites. Army Cyber Command will also ensure the

thorough follow up of any significant findings through sustained contact with the affected organizations.

In addition to influencing assessments and their results, Army Cyber Command wants to improve the integrity of its IA compliance reports and statistics, both through manual and automated means. Today, compliance reporting is largely done through semi-automated methods (e.g., machine scanning with "stubby pencil" analysis), but command emphasis is now on a fully automated reporting structure. With the enterprise tools now available to perform these scanning and reporting functions, it makes little sense to wait for the "ultimate" reporting structure. Rather, Army Cyber Command is reaching aggressively for the "low hanging fruit," things that can be leveraged today.

The Way Ahead

Standards must be clear and enforced. Discipline is a military hallmark and we must be as disciplined on our network as we are with our weapon systems. By making IA compliance a commander's priority exercised through educated users who understand their role in the defense of the network, we will better promote a strong defense of our networks.

The continued cultivation of an environment where the standard is strong compliance, the protection of information, and the guaranteed transport of information through cyberspace will make serious and lasting improvements for the security and efficiency of Army networks.

While resourcing and technical constraints deter rapid, uniform compliance, Army Cyber Command will continue to push to change the conditions

and the mindset within the Army so compliance becomes second nature.

As in any defense, adversaries will find and exploit our weakness. To counter this we must treat compliance like a weapon system and be ready to defend and protect against a threat that is real, growing and evolving. In the end, compliance with orders and directives in IA is no different than with any Army operation, task, or directive. Leaders actively engage to ensure mission accomplishment, no matter the operational domain. Maintaining the freedom to operate in cyberspace is everyone's business. Army Cyber Command is committed to supporting commands and enabling mission command.

LTC Christopher R. Quick is currently the Director of Strategic Communications for the U.S. Army Cyber Command / Second Army at Fort Belvoir, Va. His assignments include Fire Support Officer, Battery Executive Officer, Brigade Assistant Operations Officer, and Brigade Fire Direction Officer. He commanded a Battery with 1st Battalion, 17th Field Artillery. He served in the 41st Signal Battalion, 1st Signal Brigade as a Battalion Automations Officer. LTC Quick served as Brigade Information Operations Officer with the 2nd Brigade, 101st Airborne, where he served a tour in Iraq. He has served on the Army Staff within the Army G3/5/7 in DAMO-ODI and served on the Army Cyber Task Forces as the lead action officer for the development of Army Cyber Command. LTC Quick holds a B.S. degree from Park University in Kansas City, Mo. and an M.S in Computer Science and another in Information Operations from the Naval Post Graduate School in Monterey, Calif.

Certification hits the Jackpot!

*By LTC Jan C. Norris
and 1LT(P) Natasha K. Pennyfeather*

The Joint Airborne Communications Center Command Post, or more commonly called "JACKPOT," recently completed C-17 certification testing at Dover Air Force Base in late August 2012.

This milestone achievement marks a significant move toward future employment of a joint 'airborne' mission command communications capability on a larger air frame. Geographic combatant commands and other federal response agencies can now include the JACKPOT in their C-17 planning scenarios for en-route and expeditionary operations when requesting support from the Joint Communications Support Element.

The JACC-CP Echo model or "JACKPOT" was first designed in 1985 to provide mission command options to senior staffs over the battlefield or en route to a predetermined destination. The system enables key leaders to make critical decisions in the air to any ground or air unit. It consists of four pallets loaded on a C17 (or three pallets on a C-130) and is a quick loading 'roll-on roll-off' transportable platform. JACKPOT is interoperable with all DOD and civilian radio IT networks. It can support GCCs, alert postured forces, and DOD/civilian first responders. The system is scalable providing work space support for up to 16 users. During initial inception of forces, JACKPOT can enable en route mission command and planning, theater C2, airfield seizure and 'reach forward' deployment of key personnel.

The JACKPOT provides SIPR/NIPR data and secure voice services through a combination of satellite and ground based radios and associated waveforms. The international maritime satellite terminal provides 256 kilobits per second of data throughput for NIPR/SIPR, VOIP/VOSIP and multi-user internet relay chat services. In addition, JACKPOT provides access to 12-14 combat radio nets using two PSC-5s, eight PRC-117Fs (Harris Multi-Band), and four PRC-119Es. Other applications available are blue force tracker, Falconview and 'wide area voice environment' technology for radio over IP and intercom voice services. The package includes four large display monitors for viewing relevant information, data feeds or a common operating picture and each work-space houses a Microsoft Windows-based computer tablet. JACKPOT is essentially DOD's equivalent to 'wifi on-board a commercial aircraft'.

This year's C-17 certification was conducted August 20-24 at Dover Air Force Base. The event was a follow-on mitigation evaluation of the termi-

nal radio configuration test conducted last year and was executed by a group of civilian technicians subcontracted under the Air Force Research Laboratory. The primary intent of the compliance evaluation was to verify electromagnetic compatibility between the JACKPOT terminal's radio equipment and the C-17 aircraft avionics systems and specifically to re-test deficiencies found during last year's certification. The JCSE J3, J5 and 4th JCS' JACKPOT team prepared six months in advance for this year's certification by conducting radio interoperability and system checks twice a week.

Mike Ivanowicz, lead certification tester from Ball Aerospace and Technologies, said "The JACKPOT uses a lot of different radios which presents many challenges given the wide range of frequencies used. The introduction of radio frequency filters has made a significant difference for success in this year's certification.

"Our main focus is de-conflicting spectrum and mitigating any risks where JACKPOT could knock out the aircraft's GPS system," said Frank Barnhart, testing official from Select Tech. A spectrum analyzer was used to record and test all frequencies. Given the JACKPOT's unique configuration with multiple radios (14 total) transmitting simultaneously via multiple hatch mounted antennas, certifying officials also implemented tow testing by moving the C17 aircraft in various positions while validating all frequencies emitting on board the aircraft. Overall, there was significant improvement noted for this year's certification given the introduction of RF filters. Final certification approval from the Air Force C17 System Program Office and associated paperwork processing is expected within 90-120 days in the late Fall/early Winter of 2012.

The positive impacts of C17 certification are unanimous among key JCSE leaders and troops; According to MAJ(P) Bill McDowell, JCSE J3, "This certification greatly expands JCSE's ability to support Combatant Commanders and JTF commanders with an Airborne C2 capability. With C-17 certification, the operational reach and time on station is greatly expanded. Since the JACC/CP (Echo model) is currently only C-130 certified, there have been significant constraints in planning for deployment of GCC or JTF commanders, especially when forced entry opera-

tions with C-17s are the preferred airframe. "Planners will no longer have to account for the employment of a C-130 in a C-17 supported mission," added McDowell.

Bradley Smith, systems engineer for the JCSE J5 said this certification brings increased capabilities to the joint warfighter. "The C-17 certification effort is a big leap forward for enabling commander's while both en-route and within a theater of operations. The C-17 allows for the initial and return en-route missions over extended distances globally with its speed and fuel capacity," Smith stated.

SGT David Woods, JACKPOT team chief in Mike Troop, 4th JCSE said, "When conducting airborne operations on the C17, both ground troops (jumpers) and battle staff can occupy the aircraft simultaneously and this saves time and money for units conducting a mission as the aircraft lift requirement goes down. We can also use both pri-

mary and back-up power sources on the C17."

"Unlike the C-130, the C-17 has all the needed antennas pre-installed and this cuts down on set-up and installation time to get airborne and conduct operations" said SGT Anthony Matute, a JACKPOT team member.

LT(P) Natasha Pennyfeather, Mike Troop commander, 4th JCS reflected on why this year's JACKPOT re-test was successful. "The frequency of training flights increased and allowed the team to conduct more realistic testing to work through malfunctions while in the air as opposed to troubleshooting in a static ground-based setting," she stated. "Access to aircraft and 'piggy backing' off airborne operations at MacDill Air Force Base has made the difference. We also re-certified with the same AFRL test team and they were familiar with our equipment and personnel," she added.

JACKPOT is currently operated and maintained by a four

man team in 4th Squadron of JCSE at MacDill AFB, Fla. The package is typically flown and tested on a monthly basis as aircraft are available. The JACKLPOT can be loaded, configured and operational in approximately three hours for a C-17 or C-130.

During Operation Iraqi Freedom in 2006, the JACKPOT was flown in support of ground convoys for voice relay/ retransmission under the direction of USCENTCOM. More recently JACKPOT and its crew participate in the Joint Operational Airborne Exercise each year with the 82nd Airborne Division and in support of the 75th Ranger Regiment for its periodic multi-lateral training exercises. Unlike the JSTARS aircraft and systems platform, which provides similar capability, JACKPOT comes 'plug and play' ready for users and is preconfigured for quick use.

If required, the equipment can be deployed on short notice (18 hours) at the request of combatant commander's or federal agencies through a standard request process to USTRANSCOM to the Joint Enabling Capabilities Command in Norfolk, Va. to JCSE. JCSE is continually working to add capabilities as they are developed or become a requirement. In fact, the JACKPOT (fox-trot model) is being certified for use now on both C-130 and C-17 aircraft and includes improved technology and equipment.

LTC Norris is the Commander, 4th Squadron, JCSE. His most recent assignments include G6, 311th ESC (Los Angeles, Calif), Brigade S3, 516th Signal Brigade (Fort Shafter, Hawaii), and S3, 30th Signal Battalion (Wheeler Army Airfield, Hawaii).

LT(P) Natasha K. Pennyfeather is currently the Mike Troop commander in 4th Squadron, JCSE.



JACKPOT in action on board an aircraft with staff members of the Joint Enabling Capabilities Command.

CONFIGURING BATTALION FILE SERVERS

By CPT Matthew Sherburne

This is how one deploying brigade combat team filled the communications needs of its warfighters.

The 2nd Brigade Combat Team, 2nd Battalion, 325th Airborne Infantry Regiment was put on alert as a part of the Global Reaction Force following the earthquake that struck Haiti on 12 January 2010.

All of the brigade's equipment was pushed to the equipment flight line in preparation for setting up a standard Joint Network Transport Capability communications architecture at Toulouse International Airport.

Prior to the deployment, we conducted several airborne field exercises with minimal usage of the communications architecture to include digital collaboration. Services such as SharePoint, widely used in garrison, were barely used due to the low-bandwidth satellite connectivity between the battalion command post nodes and brigade JNN where the main servers are located. With no server operating system on hand, the battalion S6 shop resorted to locally sharing out folders on laptops. The main issue with this is Microsoft has a 10-user limit to accessing those shared resources on standard workstations. Furthermore, laptops are not designed to deal with the increase in data processing. Nor do they have a backup system to ensure no loss of data. Battalion-level file servers must be a Modification Table of Organization and Equipment item in order to enhance combat effectiveness and collaboration.

I joined the battalion in August 2010, just three months after returning from Operation Enduring Freedom X. Immediately I began conducting Military Decision Making Process analysis on communications support for the battalion as we prepared to head to Joint Readiness Training Center on a Forces Command tasking to validate the newest Full-Spectrum Operations Training lanes in September 2010. This became a very unique situation in which we were not allowed to bring our CPN with us because of the GRF mission. We pulled all unclassified services from the Fort Polk NEC which allowed the battalion command and staff to communicate back to Bragg and handle the usual requirement of NCOERs, OERs, and other soldier administration tasks. I realized firsthand the same issues the battalion experienced with data collaboration and file sharing in the absence of a proper file server. The interim solution I could provide as a stop gap was AKO group folders.

The automations Soldiers in the shop employed the same local folder sharing on user laptops, but again, the issue of a ten user limit became apparent when every company commander and staffer tried to access the latest OPOD documents related to the training exercise. The AKO group folders worked, but extremely slow. Ad-

ditionally, a laptop was set aside to act as a print server for the TOC printers, but the ten user limit also applied.

A month later and I found myself back out in the field for the Battalions Expert Infantryman Badge in October 2010, this time with my CPN, and this time with a file server. My S6 shop went to the Fort Bragg NEC and picked up a copy of the AGM Server 2008 to load on a Dell D630 laptop. Though not ideal, it did allow the battalion staff and command group to share files, collaborate, and print inside the Deployable Rapid Assembly Shelter.

After the EIB, I was tasked to research and design a tactical file server in preparation for our upcoming deployment to Iraq with the intent that we have it by the JRTC rotation in March 2011. Building on my past experience in Afghanistan, I knew the file servers needed to include a UPS, KVM and ruggedized transit case. The file servers themselves only needed to be fast enough to support functions in a 1U rack-mounted configuration. The UPS needed to accept 120 or 240 volts with plug adapters capable of plugging into any style plug in the world. The UPS needed to maintain power to all critical systems for a period of 15 minutes giving enough time to properly shutdown the servers in the event of a catastrophic power failure or recover from a simple tripped circuit breaker. Several months went by during the bidding process through CHESS ITES 2H and the server waiver through DA G3. Eventually DA G3/G6 granted the AKM Goal 1 Waiver and the BDE S4 completed the necessary steps for our BN S4 to purchase the file servers in May 2011. To save the Army money, I requested that Dell install major components without wiring and no operating system. I knew my automations Soldiers would be able to finish cabling the major components and install the AGM Microsoft Server 2008. The final contract included two Dell R610 1U servers with RAID 5 comprising of three 1 TB hard drives for a total of 2TB of storage on each server. Packaging Strategies, Inc installed all major components to include an APC Smart-UPS 2200VA, Paragon II P2-UMT242 42-Port, 2 User, 1U KVM Switch, P2-EUST/C Paragon II Enhanced User Station/CAC reader, Raritan 17" T1700 KVM Drawer, and two R610 servers into a 8U black double-entry case.

File-Servers arrive in Iraq

I worked an agreement with the Information Assurance department at Al Asad Air Base to place the file-servers on the strategic network. My shop kept the servers updated weekly with security patches and had zero issues with IA throughout the deployment. After a one-week validation process, my team went to work on shifting all battalion operational data from the main



This equipment was part of the 2nd Brigade Combat Team, 2nd Battalion, 325th Airborne Infantry Regiment's package shipped to operations in connections with the Global Reaction Force following the earthquake that struck Haiti on 12 January 2010.

base-wide strategic file servers to our battalion file servers. I prepared for the fact that we might jump locations after several months and wanted to make sure we were prepared to take our data with us. That moment came when the Brigade ordered our battalion to move 152 miles to Camp Taji in October 2011. At the same time the entire theater prepared to move all tactical units off strategic connectivity and onto JNTC tactical satellite assets.

This worked out perfectly because we did not need to coordinate with the Taji base network to re-establish the file-servers on their network. After setting up our CPN

on the tactical network at Taji, we connected the file-servers and had all data readily available to the battalion. We set up multiple printers through the server to expedite the establishment of the network. We setup a LAN network near as robust as the strategic network from which we left at Al Asad Air Base, Iraq. Accessing brigade shared files on their file-server connected off the JNN was so slow that it would take hours to upload one PowerPoint file. There were only a few instances in which we needed to post files on the brigade file-server so it was manageable. As for our own battalion opera-

tions, if we did not have a local file server and had to rely on the usage of the brigade file server by MTOE, our collaboration efforts would have been slowed to a crawl. Every day between October 2011 and December 2011 the command and staff utilized the file server to update Combat Update Brief slides, disseminate OPODs, and store AARs and patrol briefs.

Battalions require a file server on their local LAN both in Garrison and on deployments for rapid collaboration and continuity in data between garrison and deployment environments. With the usage of AGM Server operating systems, the Army is not spending additional money for the operating system. Less than one week of training for two 25B MOS is all that is needed for an S6 shop to adequately employ a file and print server capabilities. Maneuver battalions are constantly leveraging technology to better command and control the fight. They are keenly aware that battalions that collaborate faster and more effectively will be more successful in engaging with and destroying the enemy or conducting peacetime operations with the highest potential.

CPT Matthew Sherburne is the former battalion S6 for the 2-325 Airborne Infantry Regiment, 2BCT, 82nd Airborne Division. CPT Sherburne holds a Bachelor of Science degree in Electrical Engineering from the U. S. Military Academy.

ACRONYM QuickScan

AAAB – Al Asad Air Base, Iraq
AAR – After-Action Review
AGM – Army Gold Master
AKO – Army Knowledge Online
CPN – Command Post Node
DRASH – Deployable Rapid Assembly Shelter
EIB – Expert Infantryman Badge
FORSCOM – Forces Command
GRF – Global Reaction Force
JNN – Joint Network Node
JNTC – Joint Network Transport Capability
JRTC – Joint Readiness Training Center
KVM – Keyboard, Video, Mouse

LAN – Local Area Network
MDMP – Military Decision Making Process
MOS – Military Occupation Specialty
MTOE – Modification Table of Organization and Equipment
NEC – Network Enterprise Center
NCOER – Non-Commissioned Officer Evaluation Report
OER – Officer Evaluation Report
OPOD – Operational Order
RAID – Redundant Array of Independent Disks
TOC – Tactical Operation Center
UPS – Uninterruptible power supply

Signal classrooms embracing high-technology mobile training



By Nick Spinelli

The U.S. Army is steeped in tradition. Many of the force's actions, from ceremonies to inspections, date back centuries and are still performed as they always have been. But recently, General Dynamics' LandWarNet School on Fort Gordon broke with tradition to begin a pilot course utilizing new technologies and mobile learning in place of dated teaching methods.

"This is the Army Learning Model fully in action," said Tom Clark, the LWN Transmission Section training manager. "We can provide for Soldiers at their point of need. Every piece of the curriculum for this pilot course has been redone in the Army Learning Model format."

In the pilot course, students use tablet computers to access training materials. Content still consists of some classroom presentations, but also includes more PC-based simulations and "how-to" videos. Away from the school, they can access this same training content by going to the LandWarNet eUniversity.

"Under this program, Soldiers have a way to reach back and review content outside the classroom. Essentially, these devices double as virtual instructors," said Jarnard Gunn, one of the pilot course instructors.

Sixteen students, all under

the age of 30, make up the pilot class. Instructors believe the technological savvy typical in this age group plays a role in how the students adapt to this new learning method.

"Modern Soldiers learn differently," said Michael Wilson, a senior course instructor. "And this course helps facilitate that."

All of these students already own and use personal Smartphones and tablets. They're already familiar with the operating system. The operating system utilized is Android, which, because of its open source nature, is more adaptable to the needs of facilitators and students. However, tablet computers are only one



(Photos by Nick Spinelli/Fort Gordon Public Affairs)

SGT Kyle Weekly, a student in the General Dynamics' LandWarNet School pilot course, uses a tablet computer to scan a QR Code, accessing his training materials through the LandWarNet eUniversity.





Students attending a pilot course in General Dynamics' LandWarNet School on Fort Gordon utilize new technologies and mobile learning in place of traditional teaching methods.

part of the pilot course. Videos of Soldiers actually performing the material have replaced Power-Point presentations; and virtual references and manuals have replaced large binders of printed information. William Baker, a senior course instructor, said it's not so much a case of reinventing the wheel as motorizing it.

"Ultimately, the course is more interactive, and you see the Soldiers more interested and in-

volved than in traditional learning environments," Baker said.

An added bonus to digitizing the course is the savings involved. Nearly \$2 million in annual printing costs can now be used to provide additional training capabilities. But all the savings and ease of access are meaningless if the Soldiers don't respond well. Fortunately, that does not seem to be a problem. "I think this is definitely a step

forward," said SGT Kyle Weekly, a student in the pilot course.

"This course is allowing us to get the most cutting edge information, which I think will lead to a better end product. I'm learning the material better this way than I probably would in a traditional training environment."

Nick Spinelli is a writer/editor with the Signal Newspaper at Fort Gordon, Ga.



The Mobile User Objective System

Since the launch of the first Ultra High Frequency satellite in 1978, several replacement UHF satellite constellations have been launched as satellites neared the end of their life cycle and to support an increasing demand in UHF tactical communications.

The UHF Follow-On Constellation is the predominant constellation used by our joint warfighters around the globe today. From dismounted Special Operations Forces to the White House Communications Agency, UFO is used to provide reliable beyond line of sight connectivity in support of operations. Even though newer more capable satellites and waveforms improvements have been fielded, the overall narrowband (UHF) satellite architecture has not significantly changed in the past three decades of service.

Over the next few years, we will begin to transition to a truly new and revolutionary UHF waveform and SATCOM architecture called Mobile User Objective System. MUOS will transform the way the Department of Defense, especially the Army, uses the UHF spectrum to support military operations. MUOS is the DoD's next-generation UHF Satellite Communications system. MUOS is a next-generation narrowband tactical satellite communications system designed to significantly improve ground communications for U.S. forces on the move.

When fully deployed, MUOS will consist of four geosynchronous satellites plus an on orbit spare. These four geosynchronous satellites will provide global coverage from 65 Deg N Latitude to 65 Deg S Latitude and their orbits will provide overlapping coverage for more than seventy percent of the area. MUOS is based on a modified 3G cellular technology widely used in our



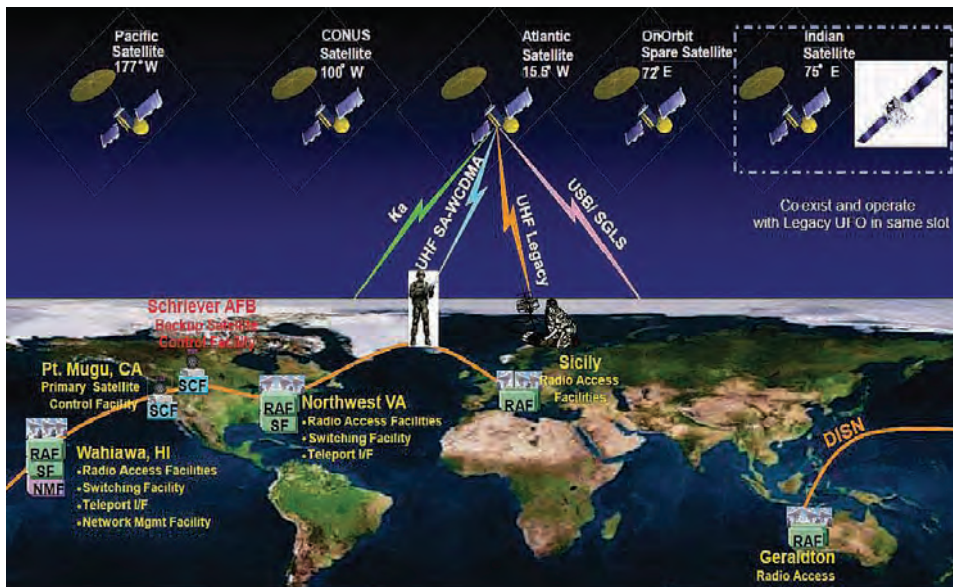
Atlas V Mobile User Objective System-1 launch, 24 February 2012

cellular phone systems of today.

There will be four ground stations to control and provision the MUOS system. MUOS operates like a global cellular service provider to support the warfighter with netted communications, cell phone-like capabilities with access to voice and data services provided by Defense Information System Network Internet Protocol based networks. It does this by adapting a Wideband Code Division Multiple Access cellular technology for

use over military UHF spectrum utilizing manpack satellite radio terminals instead of cell phones and geosynchronous satellites in place of cell towers. By operating in this portion of the spectrum, a lower frequency band than that used by conventional terrestrial cellular networks, MUOS provides warfighters the ability to operate in challenging communication environments like forested and urban areas. Users gain access to DISN provided services via gateways at the ground stations. On February 24, 2012 – The MUOS satellite was successfully launched from Cape Canaveral Air Force Station, FL, aboard a United Launch Alliance Atlas V rocket. This first MUOS satellite and associated ground system will provide initial on-orbit capability this year. The second MUOS satellite is scheduled to launch the summer of 2013, with the four-satellite global constellation achieving full operational capability by 2016. In addition to the new capabilities provided by MUOS, each satellite also has a separate legacy UHF communications payload on board to replenish and then extend the life of our current UHF narrowband communications capability until sometime past 2025. The Space and Naval Warfare Systems Command, Program Executive Office Space Systems, Communications Satellite Program Office is the program manager for MUOS.

As shown in the system architecture, there will be four active satellites on orbit around the earth, four Radio Access Facilities, two Switching Facilities – each with connectivity to a teleport, two Satellite Control Facilities and a network management facility positioned to globally support MUOS terminal users. Each MUOS satellite can view two RAFs.



MUOS Architecture

Each RAF can view two MUOS satellites via Line-of-Sight. All facilities are connected together with high-capacity terrestrial fiber. The two switching facilities route traffic through Defense Information System Agency provided teleport sites to gain access to the Global Information Grid or to the appropriate RAF facility supporting the destination terminal. The RAFs communicate the routed voice and data traffic over Ka frequency band links to the satellites. The satellites then down-convert the signals to the UHF band and transmit them to MUOS-enabled terminals via the UHF downlink.

The Signal Center of Excellence TRADOC Capability Manager for

Tactical Radios is working to bring the first MUOS-enabled terminal to our warfighters. The Joint Tactical Radio System Manpack, the AN/PRC-155, 2-channel man-packable radio will be the first ground terminal to port the MUOS waveform later this year. End-to-End MUOS testing is scheduled to begin in 2014 once the second satellite is launched and operational.

The AN/PRC-155 radio with MUOS will provide mounted and dismounted Soldiers the ability to extend operations to beyond LOS ranges while maintaining communications and situational awareness with their higher headquarters. Terminal is designed to support voice

and data rates up to 64kbps.

The MUOS-enabled tactical radio will support traditional combat nets, point-to-point communication, and point-to-network voice and data services. COL Ralph "Tripp" Higgins, TCM-TR, said "MUOS will be a game changer in terms of narrowband SATCOM capability and capacity for our Soldiers." MUOS will provide ten times the current UHF SATCOM capacity.

It is truly a global system capable of connecting any set of users regardless of their location. MUOS will offer priority-based access for assured voice and data on demand and will improve connectivity in stressed environments such as urban canyons, mountainous, jungle, weather scintillation, and provides Non-Classified Internet Protocol Router, Secret Internet Protocol Router, and Defense Switched Network access to previously disadvantaged users.

As we begin the transition from current UHF SATCOM to MUOS by deploying the system architecture and fielding our first terminal, we will expect other terminals types will certainly emerge so U.S. forces can fully leverage the potential of the game changing tactical satellite communications system known as MUOS.

Charles Schrader
TCM-TR
MUOS Lead

ACRONYM QuickScan

DISA - Defense Information System Agency
DISN - Defense Information System Network
DoD - Department of Defense
DSN - Defense Switched Network
GIG - Global Information Grid
IP - Internet protocol
JTRS - Joint Tactical Radio System
LOS - Line of Sight
MP - Manpack
MUOS - Mobile User Objective System
NIPR - Non-Classified Internet Protocol Router
PEO-Space Systems - Program Executive Office for Space Systems
RAF - Radio Access Facilities

SATCOM - Satellite Communications
SCF - Satellite Control Facilities
SF - Switching Facilities
SigCoE - U. S. Army Signal Center of Excellence
SIPR - Secret Internet Protocol Router
SPAWAR - Space and Naval Warfare Systems Command
TCM-TR - Capability Manager for Tactical Radios
TRADOC - U.S. Army Training and Doctrine Command
UHF - Ultra High Frequency
UFO - UHF Follow-On Constellation
WCDMA - Wideband Code Division Multiple Access

Joint Tactical Radio System Handheld – Manpack – Small Form Fit

The delivery of the JTRS Rifleman and Manpack Radios to the force represents the initial move to connect dismounted Soldiers on the battlefield in a net-centric way that supports the Department of Defense's movement toward network-centric operations and warfare at all tactical levels. It also signifies DOD's continued commitment to support disadvantaged warfighters.

Rifleman Radio (AN/PRC-154)

The JTRS HMS program's Milestone C Decision held on 17 June 2011 authorized an initial Low Rate Initial Production of 6,250 AN/PRC-154 Rifleman Radios and 100 AN/PRC-155 Manpack radios. On 11 July 2012, the Defense Acquisition Board chaired by Mr. Frank Kendall, Under Secretary of Defense for Acquisition, Technology and Logistics, authorized an additional LRIP of 13,077 AN/PRC-154 Rifleman Radios. It was necessary to approve an additional LRIP to allow time to review the HMS Rifleman Radio Acquisition Strategy and competition plan for Full Rate Production currently planned for 1st Quarter, Fiscal Year 2014. The DAB decision brought the total LRIP to 10% of the total planned procurement of 193,279 Rifleman Radios.

The Army's Capability Set 13

and 14 Infantry Brigade Combat Teams will start receiving Rifleman Radios in October 2012.

JTRS HMS Manpack Radio (AN/PRC-155)

The JTRS HMS MP Capability Production Document, version 2.4, was approved on 10 May 2012 via Joint Requirements Oversight Council Memorandum 067-12. The approved MP CPD supports test and evaluations and program decisions. In May 2012, the JTRS HMS Manpack Multi-Service Operational Test and Evaluation was conducted as part of the Army's Network Integration Evaluation 12.2 in White Sands Missile Range, NM. Although the HMS Manpack radio provided an operational value as a battalion and below asset capable of providing networked transport capability for Line-Of-Sight and Beyond Line-Of-Sight mission command communications, it failed to demonstrate adequate performance running the Single Channel Ground and Airborne Radio System waveform and fell short of the Manpack CPD reliability requirements. The SINCGARS waveform underwent several software updates immediately following the completion of MOT&E and a Customer Test was held 18-25 June 2012 at WSMR to characterize the SINCGARS range performance.

During the CT the Manpack radio demonstrated its ability to meet the threshold and objective SINCGARS performance requirements and showed significant improvement since MOT&E.

On 26 July 2012, an In-Progress Review DAB was conducted and chaired by USD (AT&L). The purpose of the IPR was to obtain authorization to award a contract for an additional LRIP of 3,984 AN/PRC-155 Manpack radios. The LRIPs will support Follow-on Operational Test and Evaluations and establish an initial production base to enable an orderly ramp to FRP. The DAB did not support the request for additional LRIPs. The DAB requested the Program Manager for HMS (PM-HMS) conduct a third Government Developmental Test and to return to the DAB in October 2012 with the emerging test results. The purpose of GDT 3 is to further prove out the SINCGARS' fixes and establish a greater level of confidence that a large number of the reliability challenges have been addressed appropriately. The GDT 3 will be conducted at the Electronic Proving Ground, Fort Huachuca, Ariz., 17-28 September 2012.

Joseph Bailey
Janus Research Group
Senior Systems Engineer

ACRONYM QuickScan

AS - Acquisition Strategy
BLOS - Beyond Line of sight
CPD - Capability Production Document
CS - Capability Set
CT - Customer Test
DAB - Defense Acquisition Board
FOT&E - Follow-on Operational Test and Evaluations
FRP - Full Rate Production
GDT3 - Government Developmental Test
IBCT - Infantry Brigade Combat Teams
IPR - In Progress Review
JROCM - Joint Requirements Oversight Council

Memorandum
JTRS - Joint Tactical Radio System
LOS - Line of Sight
LRIP - Low Rate Initial Production
MOT&E - Multi-Service Operational Test and Evaluation
RR - Rifleman Radios
SINCGARS - Single Channel Ground and Airborne Radio System
USD AT&L - Under Secretary of Defense for Acquisition, Technology and Logistics
WSMR - White Sands Missile Range

Are you sure the network is protected?



LWNeU is your Government resource for Network , Systems, COMSEC, Security Training and Information



LWN.ARMY.MIL
LandWarNet eUniversity

LANDWARNET
eUNIVERSITY

Everything

Use quotes to narrow search results

[Home](#) | [Unit Universities](#) | [Training](#) | [Downloads](#) | [LWNeU Forums](#) | [Video Training](#) | [Doctrine](#) | [Support](#)

[LandWarNet eUniversity](#) > [Home](#)

LWNeU Resources

- [Blackboard 7](#)
- [Blackboard 9](#)
- [FORSCOM C4 Training Wiki](#)
- [My Communities](#)

Signal Resources

- [Signal Knowledge Network](#)
- [Signal Link](#)
- [S6 Community of Purpose](#)
- [Signal Lessons Learned](#)
- [WIN-T Gateway](#)

Additional Resources

- [AKO/DKO](#)
- [Information Assurance Training](#)
- [Army Training Net](#)
- [Digital Maintenance](#)

**Get
Training**

[SEARCH FOR TRAINING](#)

[BROWSE WIKIS](#)

[UNIT UNIVERSITIES](#)

» **TRC 170A TROPO IMI**
» **PHOENIX AN/TSC DELTA**
» **25P10 IMI**

NEW SIMS

New BCCS Training



New on-line training available for CPOF on LWNeU

The Command Post of the Future (CPOF) Interactive Multimedia Instruction (IMI) courses provide computer-based training for both CPOF operators and system

Training Spotlight



New on-line training and information for Tactical Electric Power systems

- Tactical Quiet Generators
- Advanced Medium Mobile Power Sources (AMMPS)
- Improved Environmental Control Unit (IECU)

- Power Distribution Illumination Systems Electrical (E)

line train available.

Find What You Are Looking For....

Lwn.army.mil

DEPARTMENT OF THE ARMY
ARMY COMMUNICATOR
USASC&FG
ATTN: ATZH-POM
Fort Gordon, Georgia 30905-5301

PERIODICALS
Postage and fees paid
at Augusta, Georgia and
additional cities

OFFICIAL BUSINESS
ISSN 0362-5745

*"Always continue the climb.
It is possible for you to do
whatever you choose, if you
first get to know who you
are and are willing to work
with a power that is greater
than ourselves to do it."*

- ELLA WHEELER WILCOX
AMERICAN AUTHOR

SGM Michelle Peters

VI CAREER MANAGER
OFFICE CHIEF OF SIGNAL
USASIGCoE and FORT GORDON

*The next edition of the
Army Communicator
offers a look at where some
Signal careers have come
from and where they are
headed in the massive
Signal transformation
that is underway.*

**ARMY
COMMUNICATOR**

Signal Towers, Room 713
Fort Gordon, Georgia 30905-5301
PIN: 103093-000

